DESENVOLVIMENTO DE UMA APLICAÇÃO PARA CRIPTOGRAFIA DE TEXTOS E ARQUIVOS DE TEXTO

BATTISTI, José Henrique[1]
j0se.henrique@hotmail.com
DEZENGRINI, Elenilton Jairo[2]

RESUMO

Este artigo tem por objetivo o desenvolvimento de uma aplicação para a criptografia de textos e arquivos de texto. Nele, apresenta-se um pouco da história da criptografia, assim como a importância da mesma na atualidade. Explicando ainda sobre criptografias de chaves simétricas e assimétricas, expondo alguns métodos. A aplicação levou em consideração a confidencialidade e o sigilo dos dados para atender às necessidades básicas de um usuário, que busca sigilo em suas informações. Para o desenvolvimento desta aplicação foi utilizada a linguagem de programação Java e a interface de desenvolvimento integrada Eclipse - IDE. Os resultados obtidos neste artigo mostram o quão importante é a criptografia, para a segurança da informação enfatizando ainda mais a necessidade e eficiência na proteção de informações pessoais e corporativas.

PALAVRAS-CHAVE: Criptografia, Informação, Segurança, Sigilo.

1 INTRODUÇÃO

Em tempos antigos, as comunicações entre povos distantes se davam através de mensagens escritas. Temendo a interceptação por outras pessoas, com o passar dos anos, foram desenvolvidas diversas técnicas para a ocultação de mensagens através de cifras ou códigos secretos (SILVA, 2006).

A criptografia utiliza métodos e técnicas para modificar mensagens, tornando-as de difícil compreensão, de forma que apenas o legítimo destinatário consiga decifrá-la, conseguindo assim, o acesso à informação original (FARIA, 2006).

A proposta se justifica, pois, com o avanço constante da tecnologia, o mundo está se tornando cada vez menor e sem fronteiras, sendo que, com apenas um clique, é possível enviar informações em questão de minutos ou até mesmo segundos. Este avanço torna a informação e o controle sobre ela extremamente importantes para o governo e as empresas. Quanto maior o fluxo e a quantidade de informações na rede, maior será a necessidade das organizações, governos e até pessoas comuns buscarem uma proteção contra uma nova

[1] Discente do Curso de Sistemas de Informação do Centro Universitário Assis Gurgacz.
[2] Docente orientador – Centro Universitário Assis Gurgacz Curso de Sistemas de Informação.

ameaça, a qual cresce a cada dia, junto ao desenvolvimento da tecnologia. Trata-se do roubo de informações estratégicas e sigilosas, armazenadas na rede computacional.

Tendo em mente a necessidade de criação de ferramentas capazes de proteger a informação e garantir segurança aos dados armazenados e enviados pelas organizações ao redor do mundo, se comprova a motivação para o estudo da criptografia, buscando criar uma aplicação que dê maior segurança aos dados digitais.

Diante do tema proposto, os objetivos envolveram o desenvolvimento de algoritmos de criptografia através de programação em Java, como uma forma de mascarar uma mensagem, de maneira que somente a pessoa autorizada poderá ter acesso ao seu conteúdo.

2 REVISÃO BIBLIOGRÁFICA

Criptografia ou Criptologia, "*Cripto*" vem do grego "*kryptós*" que significa oculto, escondido, e "grafia" também do grego "*gráphein*" significa escrever. A criptografia em si, estuda os métodos para codificar ou cifrar determinada informação, de modo que somente o proprietário ou o legítimo destinatário seja capaz de interpretar e visualizar o conteúdo da informação, sendo ilegível para intrusos ou terceiros (COUTINHO, 2008).

A criptografia está presente desde antes de Cristo, seu progresso é apontado em três grandes períodos: artesanal, mecânico e digital (SINGH, 2008). O período artesanal se manifestou paralelamente ao surgimento da escrita, durante as idades antiga e média, quando a utilização era feita com lápis e papel, o que tornava fácil a decifração (KAHN, 1996). Já o período mecânico, se iniciou na idade moderna, a partir da Revolução Industrial, quando as máquinas surgiram no mundo, tendo seu auge na Segunda Guerra Mundial, sendo possível verificar o avanço das máquinas para criptografar mensagens (DIFFIE e HELLMAN, 1976).

Por fim, o período digital surgiu, e com o avanço dos computadores, realizando cálculos extremamente grandes em um pequeno intervalo de tempo, tornando-se uma ferramenta valiosa na criptografia (SINGH, 2008).

Para Diffie e Hellman (1976, p. 645), "a criptografia é o estudo de sistemas "matemáticos" envolvendo dois tipos de problemas de segurança: privacidade e autenticação".

Já Singh (2008) define a criptografia como a união de funções e técnicas que transformam informações em dados codificados, convertendo textos legíveis em ilegíveis.

Atualmente, a criptografia é utilizada para fins "não militares", sem que seja percebido. As transações bancárias que nos habituamos a fazer, não dispensam rigoroso

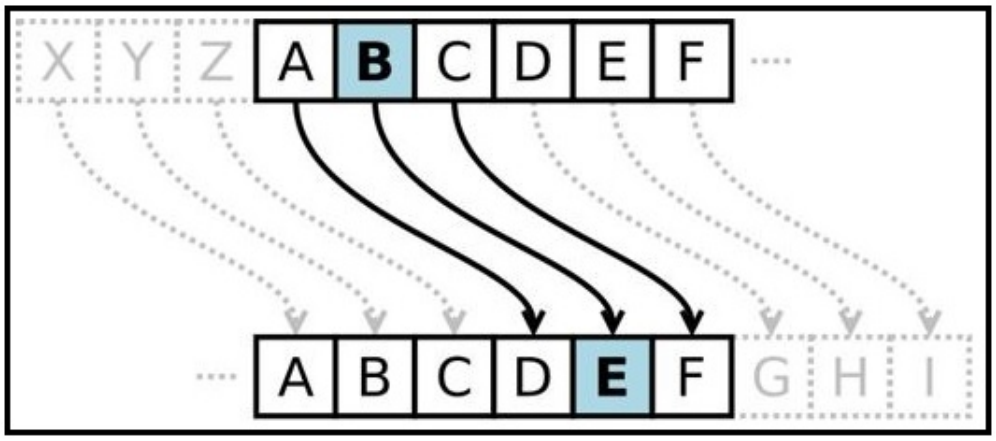
sistema de segurança em que se utiliza a criptografia. A mesma técnica utilizada por algumas emissoras de TV por assinatura, que codificam o sinal, para que somente seus assinantes, portadores de aparelhos decodificadores, possam assistir às imagens por elas transmitidas.

A cada dia, toda a segurança das atividades desenvolvidas através da Internet está dependendo de fórmulas criptográficas eficientes e seguras. Transações eletrônicas por meio de cartões de crédito, operações *home-banking,* e até mesmo dinheiro digital, tem sua segurança fundada em um complexo sistema criptográfico, de modo que o uso de criptografia forte tem se mostrado requisito essencial para o desenvolvimento do comércio eletrônico. Igualmente, o sigilo de nossa correspondência eletrônica só é possível com a utilização desta técnica (MARCACINI, 2010).

2.1 CIFRA DE CÉSAR

A primeira cifra que é conhecida no mundo ocidental é a cifra de César. Como todas as cifras antigas, ela realiza a substituição monoalfabética. O método da cifra move cada letra do alfabeto três posições para a direita, de acordo com o alfabeto da língua (Figura 1) (ZOCHIO, 2016).

Figura 1 – Funcionamento da Cifra de César



Fonte: Setesys (2012)

Utilizando o método acima, podemos trazer o exemplo da Figura 2.

Figura 2 – Exemplo da Cifra de César

O texto original "Artigo Criptografia" ao ser criptografado com a cifra de César, ficaria:

DUWLJRFULSWRJUDILD

Fonte: Elaborado pelo autor. Adaptado de Stallings (2008).

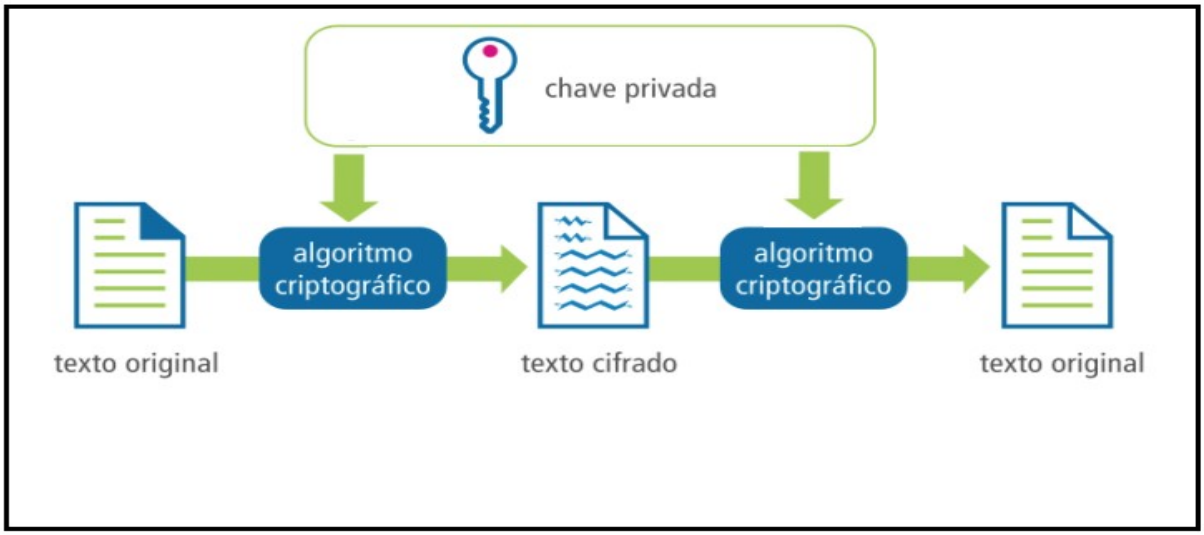
2.2 MECANISMOS CRIPTOGRÁFICOS

Os mecanismos criptográficos são capazes de garantir a segurança e confidencialidade, pois, uma vez encriptados, somente o proprietário da chave correta poderá decriptá-los e ter acesso à informação, sendo divididos em dois principais tipos, de acordo com a função das chaves que operam, são elas: chaves simétricas e chaves assimétricas, as quais serão descritas a seguir (WYKES, 2016).

2.2.1 Chaves Simétricas

As chaves simétricas também são conhecidas como criptografia de chave privada (Figura 3), utilizada desde a década de 70, e considerada a maneira mais convencional de criptografia, baseia-se na utilização de um algoritmo matemático com uma chave, que é utilizada para ambas as funções, criptografar e decriptografar (ZOCHIO, 2016).

Figura 3 – Funcionamento da criptografia por chave simétrica



Fonte: Elaborado pelo autor. Adaptado de Macêdo (2011).

A criptografia de chave simétrica usa uma única chave, para cifra de dados, e posteriormente para decifrá-la. Isso impõe uma restrição aos cenários que envolvem duas ou mais partes, cada parte necessita obrigatoriamente possuir a mesma chave (WYKES, 2016).

Marcacini (2010) comenta sobre as limitações na criptografia simétrica:

> [...] mesmo como método de segurança na comunicação, a criptografia simétrica padece de limitações. De um lado as partes devem ter, ao menos uma vez, um meio seguro de comunicação para combinar as chaves secretas. E isso nem sempre é possível. De outro lado, se quisermos manter conversações sigilosas com diversas pessoas, teremos que combinar uma chave diferente para cada uma delas, a menos que todas façam parte de um mesmo grupo e possam ter acesso a todas as informações que circulem entre elas. Do contrário, a chave passará a ser conhecida por um grande número de pessoas, em prejuízo de sua segurança (MARCACINI 2010, p. 30).

Abaixo é possível evidenciar a quantidade de combinações possíveis de acordo com o tamanho da chave em bits (ZOCHIO, 2016).

- Chave de 4 bits = 16 chaves possíveis.
- Chave de 56 bits = 72.057.594.037.927.936 chaves possíveis.
- Chave de 128 bits = 340.282.366.920.938.463.374.607.431.768.211.456 chaves possíveis.

Levando em consideração que, quanto maior o tamanho da chave, maior será a dificuldade em se obter o resultado.

2.2.1.2 *Data Encryption Standard (DES) e 3-DES*

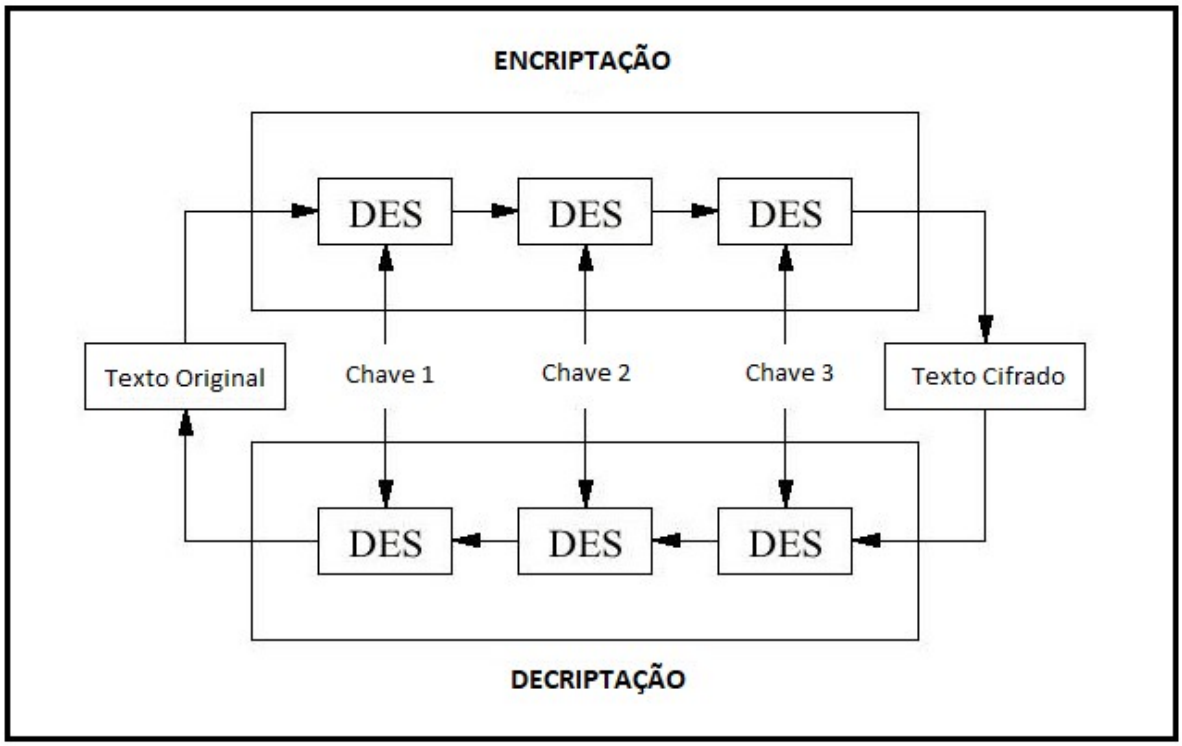
O modelo de criptografia mais empregado no esquema de chaves simétricas é baseado na *Data Encryption Standard* (DES), desenvolvido pela *International Business Machines* (IBM) em 1977. Seu objetivo é que seja difícil o cálculo da chave, pois mesmo tendo conhecimento do algoritmo, a mensagem original é a mensagem cifrada (STALLINGS, 2008).

O modo de funcionamento deste modelo é a codificação dos dados em blocos de 64 bits com uma chave de 56 bits. O algoritmo transforma a entrada de 64 bits em uma série de saída também de 64 bits. O mesmo processo, com as mesmas etapas e com a mesma chave, será utilizado para reverter a codificação (BRAZIL, 2007).

Devido ao avanço do processamento computacional, um ataque de força bruta se tornou algo possível de ocorrer, visto que sua chave possui apenas 56 bits, para esta possibilidade, o algoritmo 3-DES ou *triple-DES,* foi desenvolvido, para garantir uma maior

segurança do algoritmo DES. Basicamente o 3-DES (Figura 4) aplica o algoritmo DES por três vezes consecutivas, cada vez com uma chave distinta, onde ambas atuam como uma única chave, com tamanho de 192 bits (WYKES, 2016).

Figura 4 – Funcionamento método 3-DES



Fonte: Elaborado pelo autor. Adaptado de Cheung (2002).

2.2.2 Chaves Assimétricas

Mais conhecida como criptografia de chave pública, algoritmos com chave assimétrica apontam uma grande melhora e solução para o problema do compartilhamento de chave encontrada na criptografia simétrica. Este modelo utiliza duas chaves, sendo uma chave denominada de privada e a outra de pública. A chave pública é acessível a todos que desejam se comunicar de modo seguro, enquanto a privada é conhecida somente por seu respectivo dono. Com ambas as chaves, se torna possível decifrar uma mensagem criptografada (VOITECHEN, 2015).

A fim de entender o conceito, Oliveira (2012) diz que:

> [...] basta pensar num cadeado comum protegendo um determinado bem. A mensagem é este bem, e o cadeado, que pode ficar exposto, é a chave pública. Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem. A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada (OLIVEIRA, 2012, p.4).

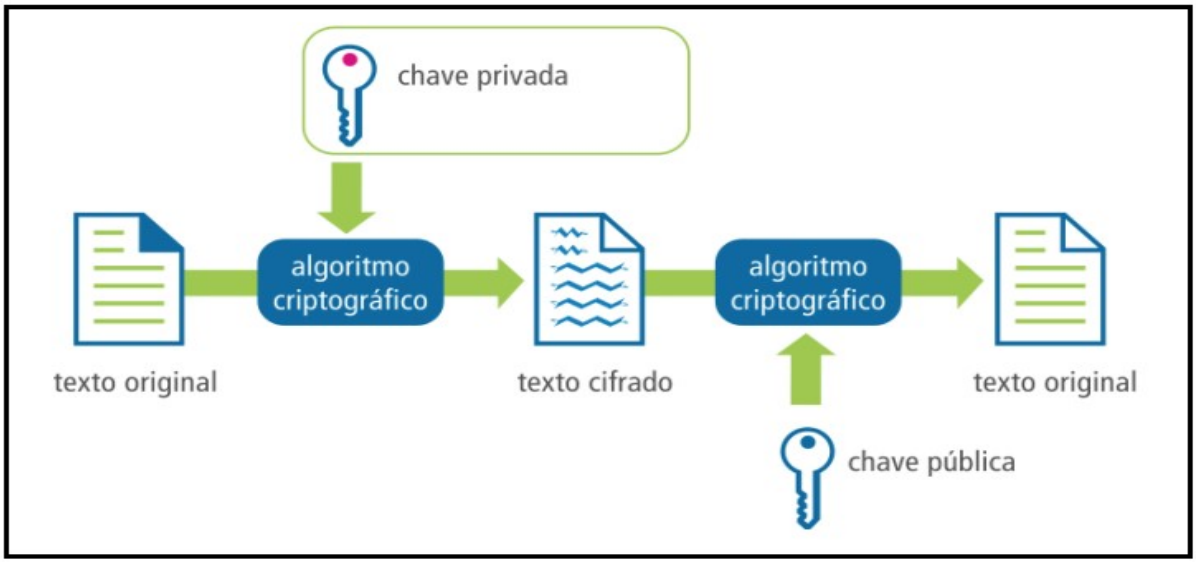
A vantagem deste método é o não compartilhamento de chaves privadas, no entanto, o seu ponto fraco se deve ao fato de que o tempo de processamento é elevado em comparação à criptografia simétrica, o que em muitos casos torna sua utilização inviável.

"O algoritmo assimétrico minimiza o problema de troca de chaves, pois não é necessário um canal seguro para tal. Porém, ele é cerca de 60 a 70 vezes mais lento que os algoritmos simétricos (NAKAMURA e GEUS, 2007, p. 304) ".

O esquema de criptografia de chave pública (Figura 5) ou assimétrica, descrito por Stallings (2008), possui os seguintes métodos:

- Texto claro: Mensagem ou dado legível que serão inseridos no algoritmo.
- Algoritmo de criptografia: O algoritmo irá realizar a transformação do texto claro.
- Chave pública e privada: O par de chaves utilizadas, de modo que a chave privada será usada para criptografar, e a chave pública para decriptografar.
- Texto cifrado: Será a mensagem codificada, produzida pelo algoritmo, dependerá do texto claro e de ambas as chaves.
- Algoritmo de decriptografia: O algoritmo irá aceitar o texto cifrado, e junto com as chaves correspondentes, irá transformar o texto novamente em texto claro (STALLINGS, 2008).

Figura 5 – Funcionamento da criptografia por chave assimétrica



Fonte: Elaborado pelo autor. Adaptado de Macêdo (2011).

2.2.2.1 RSA

A partir da criação do método de criptografia com chave pública, houve busca por um modelo de criptografia assimétrica, Rivest, Shamir e Adleman, em 1978, desenvolveram um novo método de criptografia, denominada RSA (*Rivest-Shamir-Adleman*), utilizando números inteiros, que foi desenvolvida por grandes matemáticos, como Fermat, Euler, Gaussacc. Nesta criptografia, as chaves privadas e públicas são compostas por dois números naturais cada (e, n) e (d, n), onde ‘n’ é o produto de dois números primos, ‘e’ e ‘d’. Para obter a chave privada a partir da chave pública, basta realizar a fatoração do número natural ‘n’. Assim, aparenta ser um processo fácil "quebrar" a criptografia RSA, porém, na prática isso é extremamente difícil (CASTRO, 2014).

O argumento por trás do RSA, resume-se na facilidade de multiplicação de dois números primos para adquirir um terceiro número, porém é muito custoso de recuperar os dois primos a contar daquele terceiro número. Isto é conhecido como fatoração. Digamos que, os fatores primos de 3.337 são 71 e 47. Gerar sua chave pública envolve multiplicar dois primos grandes. Formar a chave privada a partir da pública implica na fatoração de um grande número, logo a segurança do RSA se dá pela dificuldade de fatoração de grandes números (OLIVEIRA, 2012).

Para demonstrar o funcionamento do algoritmo RSA, segundo Stallings (2008), se utiliza números primos (P e Q). Para exemplificar essa situação, o autor define dois números primos:

$$P = 17$$
$$Q = 11$$

De acordo com P e Q, vamos calcular dois novos primos N e Z

$$N = P * Q$$
$$Z = (P - 1) * (Q - 1)$$

Desta maneira, obtemos o resultado:

$$N = 17 * 11 = 187$$
$$Z = (17 – 1) * (11 – 1) = 160$$

Determinando um número D, também primo em relação à Z decide-se:

$$D = 7$$

Após a definição dos valores acima, são criadas as chaves públicas e privadas. Assim, se procura o valor de E para seguinte operação:

$$(E * D) \bmod Z = 1$$

Definindo os valores de testes em 1, 2 e 3... dispomos de:

$$E = 1 => (1*7) \bmod 160 = 7$$
$$E = 2 => (2*7) \bmod 160 = 14$$
$$E = 3 => (3*7) \bmod 160 = 21$$
$$E = 23 => (23*7) \bmod 160 = 1$$
$$E = 183 => (183*7) \bmod 160 = 1$$
$$E =343 => (343*7) \bmod 160 = 1$$

Assim, se encontram os números 23, 183 e 343 que correspondem à propriedade indicada, para simplificar a operação, usaremos:

$$E = 23$$

Criptografar: E e N – serão a chave pública;
Decriptografar: D e N – serão a chave privada.

Sendo assim:

$$\text{TEXTO CRIPTOGRAFADO} = (\text{TEXTO ORIGINAL } E) \bmod N$$
$$\text{TEXTO ORIGINAL} = (\text{TEXTO CRIPTOGRAFADO } D) \bmod N$$

Se o texto definido for o número 4

Criptografando:

TEXTO ORIGINAL = 4
TEXTO CRIPTOGRAFADO = (4 ^ 23) mod 187
TEXTO CRIPTOGRAFADO = 70.368.744.177.664 mod 187
TEXTO CRIPTOGRAFADO = 31

Decriptografando:

TEXTO RECEBIDO = 64
TEXTO ORIGINAL = (64 ^ 7) mod 187
TEXTO ORIGINAL = 4.98.046.511.104 mod 187
TEXTO ORIGINAL = 4

Apesar do exemplo acima utilizar números primos pequenos, é crucial a utilização de números primos gigantescos, haja vista que, quanto maior o número, maior é o tempo de cálculo das equações (STALLINGS, 2008).

3 PROCEDIMENTOS METODOLÓGICOS

Para a execução deste trabalho, foi aplicada a linguagem de programação Java para o desenvolvimento dos algoritmos, e para manipulação da linguagem, foi utilizado o ambiente de desenvolvimento integrado Eclipse – IDE, que fornece os recursos necessários para o desenvolvimento dessa aplicação, esse software recebe o nome de *Crypto*.

Neste artigo se optou pela metodologia de pesquisa bibliográfica utilizando-se livros e artigos, com abordagem de investigação qualitativa em relação aos resultados, uma vez que, a aplicação busca assegurar o sigilo das informações. A realização da pesquisa bibliográfica é de grande importância para que se tenha conhecimento teórico, e desta forma seja possível analisar as principais contribuições teóricas sobre um tema ou assunto específico (KÖCHE, 2011).

A pesquisa qualitativa possui aspectos essenciais que consistem em escolher adequadamente os métodos e teorias para o reconhecimento e análise de perspectivas distintas, para assegurar o processo de conhecimento do assunto abordado (FLICK, 2009).

Com base nos métodos de criptografia simétrica, foi desenvolvida uma aplicação utilizando parte dos conceitos teóricos já existentes com a linguagem de programação Java, cuja finalidade busca garantir o sigilo e a segurança da informação.

3.1 Contagem dos caracteres

Ao efetuar uma entrada de caracteres na interface da aplicação, são realizadas algumas validações, as quais serão fundamentais para a execução. Ao digitar ou localizar o texto, é realizado o "*SIZE"* total dos caracteres, tendo o valor, será atribuída uma contagem de zero (0) a quatro (4), sendo '*SIZE*" zero (0) a quantidade de zero (0) a nove mil (9000) caracteres e a quatro (4) de 9.999,000 a 99,999.000 (Figura 6).

- SIZE_ZERO de 0 à 9.000 caracteres.
- SIZE_ONE de 9.000 a 90.000 caracteres.
- SIZE_TWO de 90.000 a 999.000 caracteres.
- SIZE_THREE de 999.000 a 9.999.000 caracteres.
- SIZE_FOUR de 9.999.000 a 99.999.000 caracteres;

Figura 6 – Contagem de caracteres

```
SIZE_ZERO(9_000),
SIZE_ONE(90_000),
SIZE_TWO(999_000),
SIZE_THREE(9_999_000),
SIZE_FOUR(99_999_000),
```

Fonte: Elaborado pelo autor (2018).

3.2 Criação da Chave

Tendo o tamanho da contagem dos caracteres, o algoritmo segue para o próximo passo, que é a geração de uma chave aleatória para a execução do algoritmo. Esta chave está definida por *default* com 20 caracteres, exceto quando a contagem de caracteres for menor que 20, neste caso, a chave terá o mesmo tamanho que o texto.

3.3 Criação da Interface MAP – JAVA

Após os passos anteriores serem executados, o MAP inicia a definição dos caracteres em números, esta definição será realizada iniciando pelo primeiro valor da chave, seguindo para o primeiro valor do texto, e assim sucessivamente.

Se utilizarmos o Texto sendo “OLA” e a chave sendo “H1B” teríamos o seguinte MAP:

Chave1: 0001 = H

Texto1: 0002 = O

Chave2: 0003 = 1

Texto2: 0004 = L

Chave3: 0005 = B

Texto3: 0006 = A

3.4 Criptografia dos dados

Com os valores do MAP, será iniciada a criptografia do texto, que se resume através de operações matemáticas de soma.

Chave1: 0001 + Texto1: 0002 + PosiçãoTexto = 0004 → O

Chave2: 0003 + Texto2: 0004 + PosiçãoTexto = 0009 → L

Chave3: 0005 + Texto3: 0006 + PosiçãoTexto = 0014 → A

Após esta operação teríamos o texto “OLA” convertido para 000400090014.

3.5 Decriptografia de Dados

No momento da decriptografia dos dados, a operação inversa é realizada, e o primeiro valor do Texto é subtraído pelo primeiro valor da chave, subtraída novamente pela posição original do texto.

0004 – Chave1: 0001 – PosiçãoTexto = 0002 → O

0009 – Chave2: 0003 – PosiçãoTexto = 0004 → L

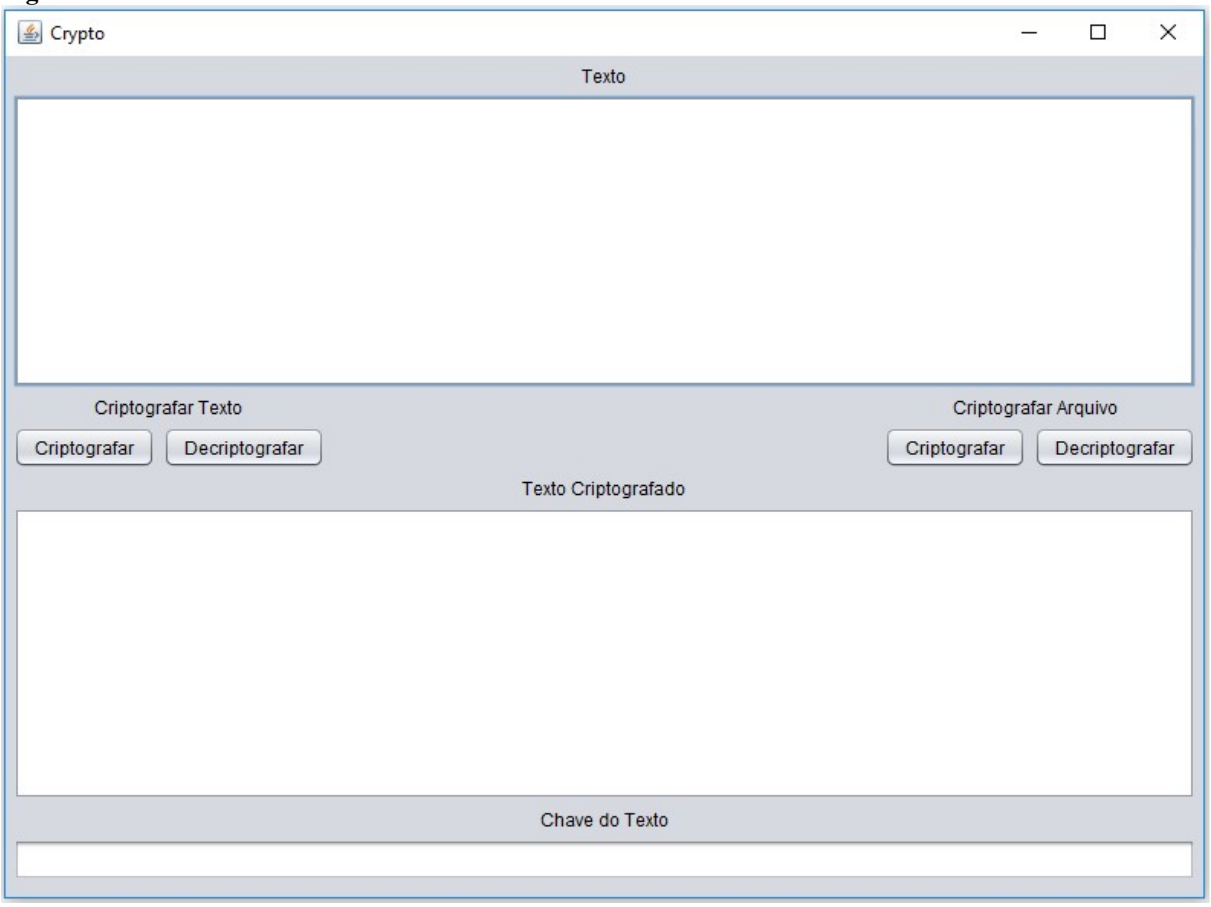
0014 – Chave3: 0005 – PosiçãoTexto = 0006 → A

4 RESULTADOS E DISCUSSÃO

O resultado deste artigo é um *software* com o intuito de garantir a segurança e sigilo das informações, através de criptografia. Esse *software* recebe o nome de *Crypto.*

O *software* foi testado, garantindo seu funcionamento através de simulações. Ao abrir o arquivo executável, apresenta-se a tela do programa com os campos: "**Texto**", "**Texto Criptografado**" e "**Chave do Texto**" em branco, juntamente com duas operações, "**Criptografar Texto**" e "**Criptografar Arquivo**", há dois botões em cada operação, sendo eles: "**Criptografar**" e "**Decriptografar**" (Figura 7).

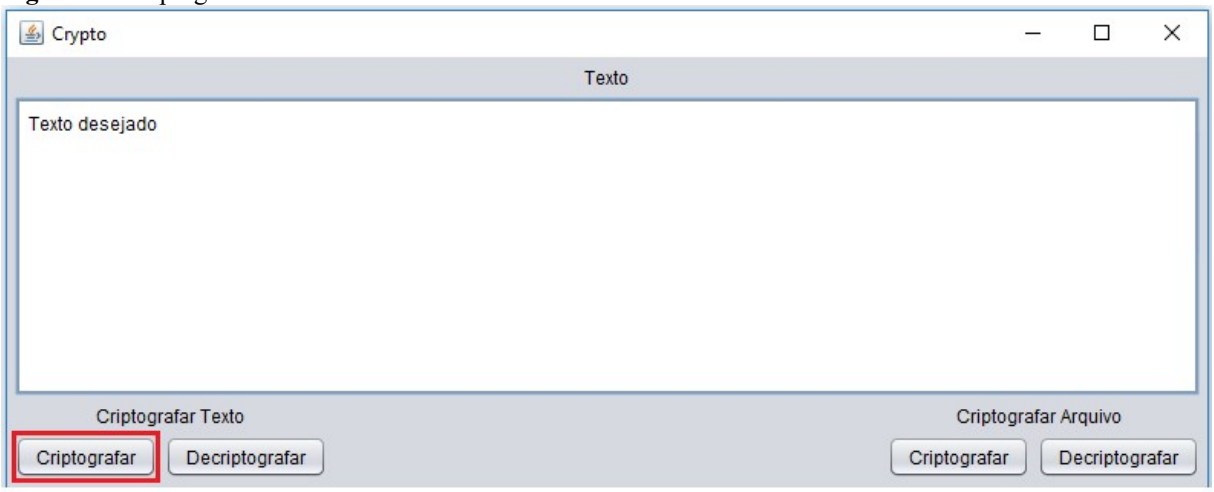
Figura 7 – Tela inicial



Fonte: Elaborado pelo autor (2018).

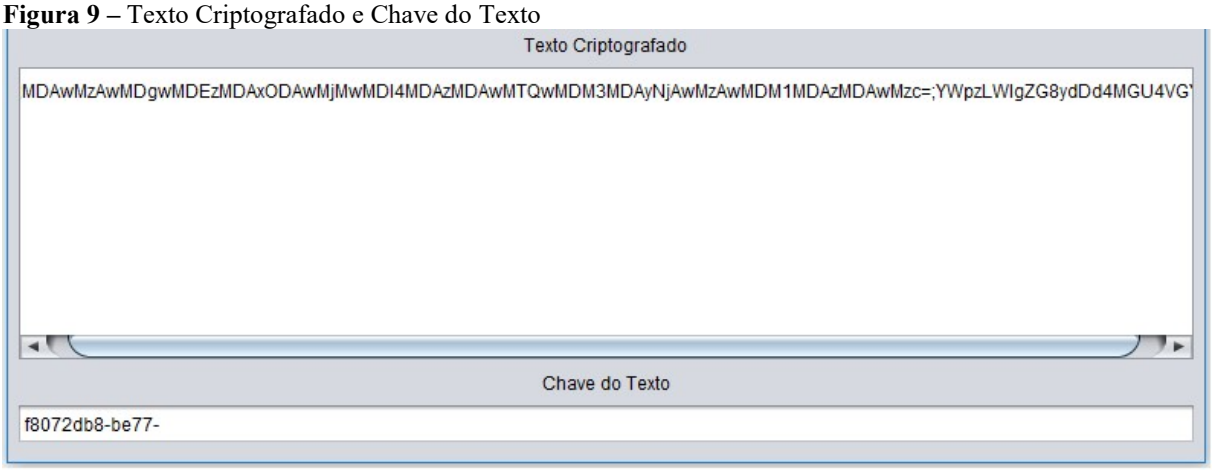
O utilizador irá digitar o texto desejado ou selecionar o arquivo de texto procurado. Caso opte pela primeira opção, após inserir o texto no campo informado, ao clicar no botão "**Criptografar**" da operação "**Criptografar Texto,** " o programa irá executar a criptografia, gerando o texto criptografado e a chave do texto (Figura 8 e 9).

Figura 8 – Criptografando texto



Fonte: Elaborado pelo autor (2018).

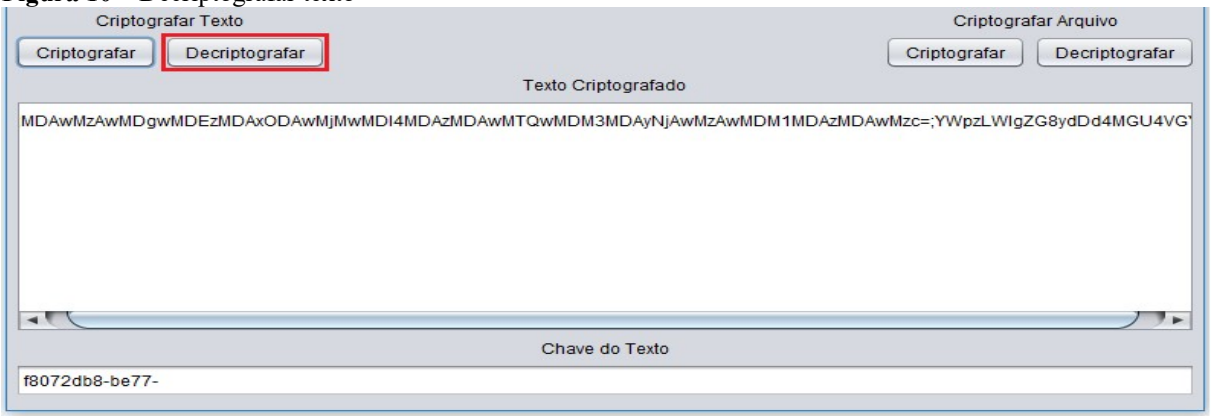
Figura 9 – Texto Criptografado e Chave do Texto



Fonte: Elaborado pelo autor (2018).

Neste momento, o usuário está de posse do texto criptografado e de sua respectiva chave, caso alguma informação de qualquer um dos campos seja alterada, a decriptografia será inexecutável. Porém, com ambas as informações inseridas em seus respectivos campos, ao clicar no botão "**Decriptografar**" da operação "**Criptografar Texto**", o usuário conseguirá visualizar o texto original, sem a criptografia (Figura 10).

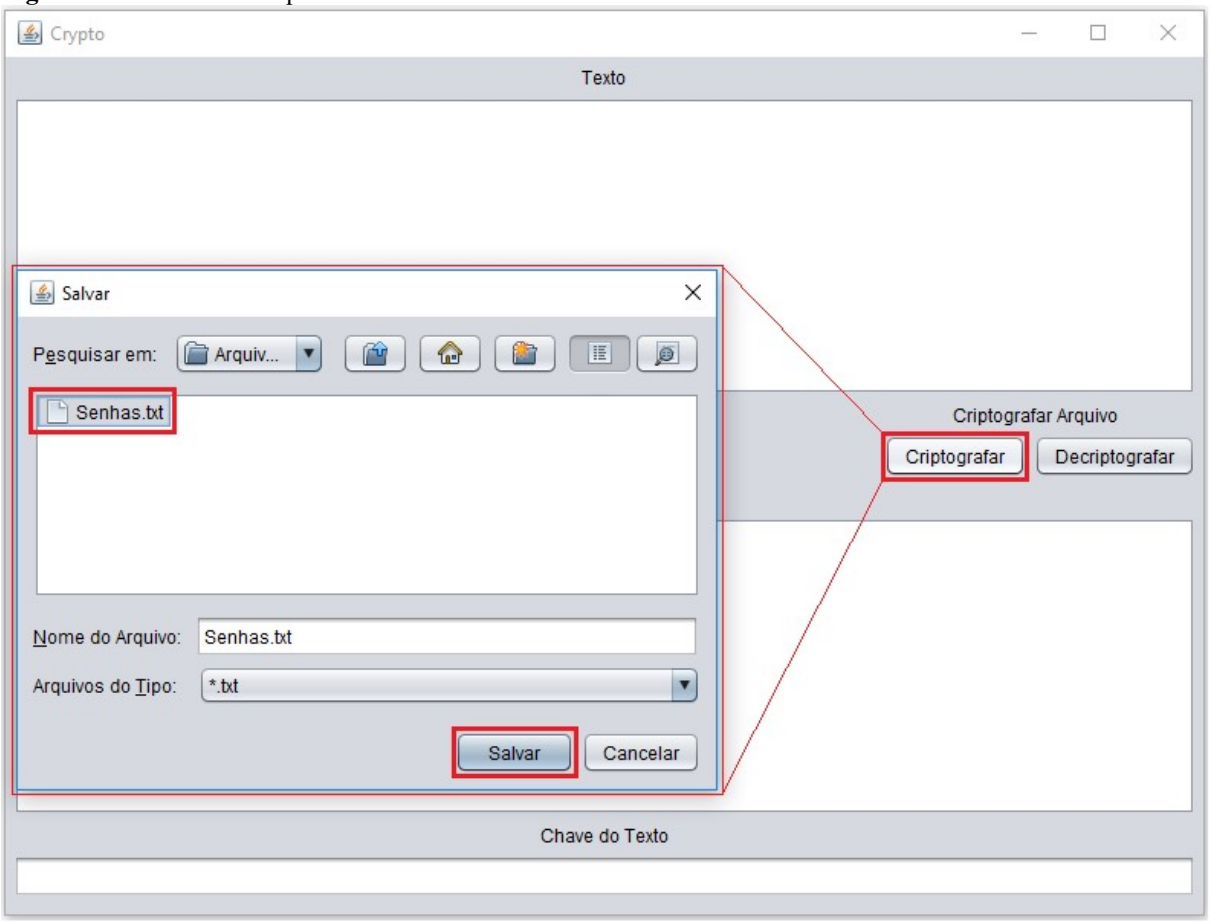
Figura 10 – Decriptografar texto



Fonte: Elaborado pelo autor (2018).

No entanto, se o usuário optar por selecionar o arquivo, ao clicar no botão "**Criptografar**" da operação "**Criptografar Arquivo**" será aberta a tela de busca do arquivo, onde deverá ser localizado o arquivo.txt, no diretório específico (Figura 11).

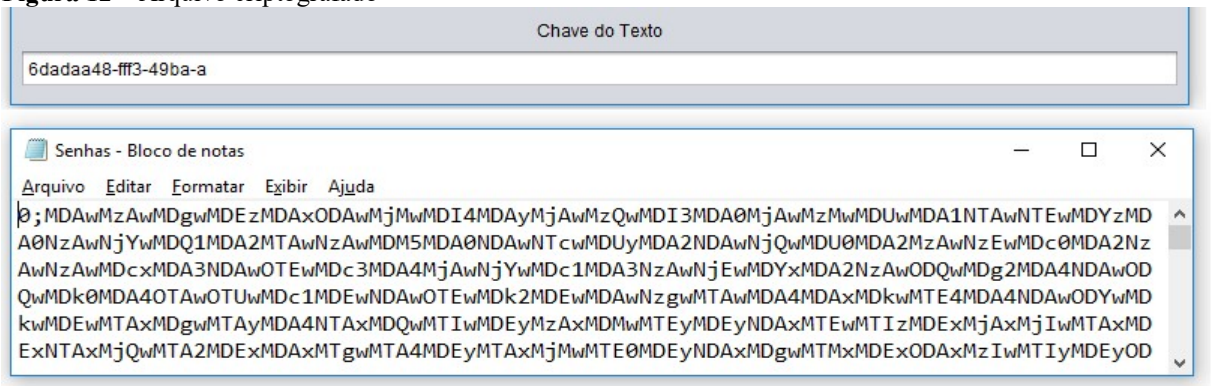
Figura 11 – Selecionar arquivo



Fonte: Elaborado pelo autor (2018).

Após selecionar o arquivo de texto desejado, o processo de criptografia será iniciado, alterando o conteúdo do arquivo pelo texto criptografado, e enviando a chave no campo "**Chave do Texto**" (Figura 12).

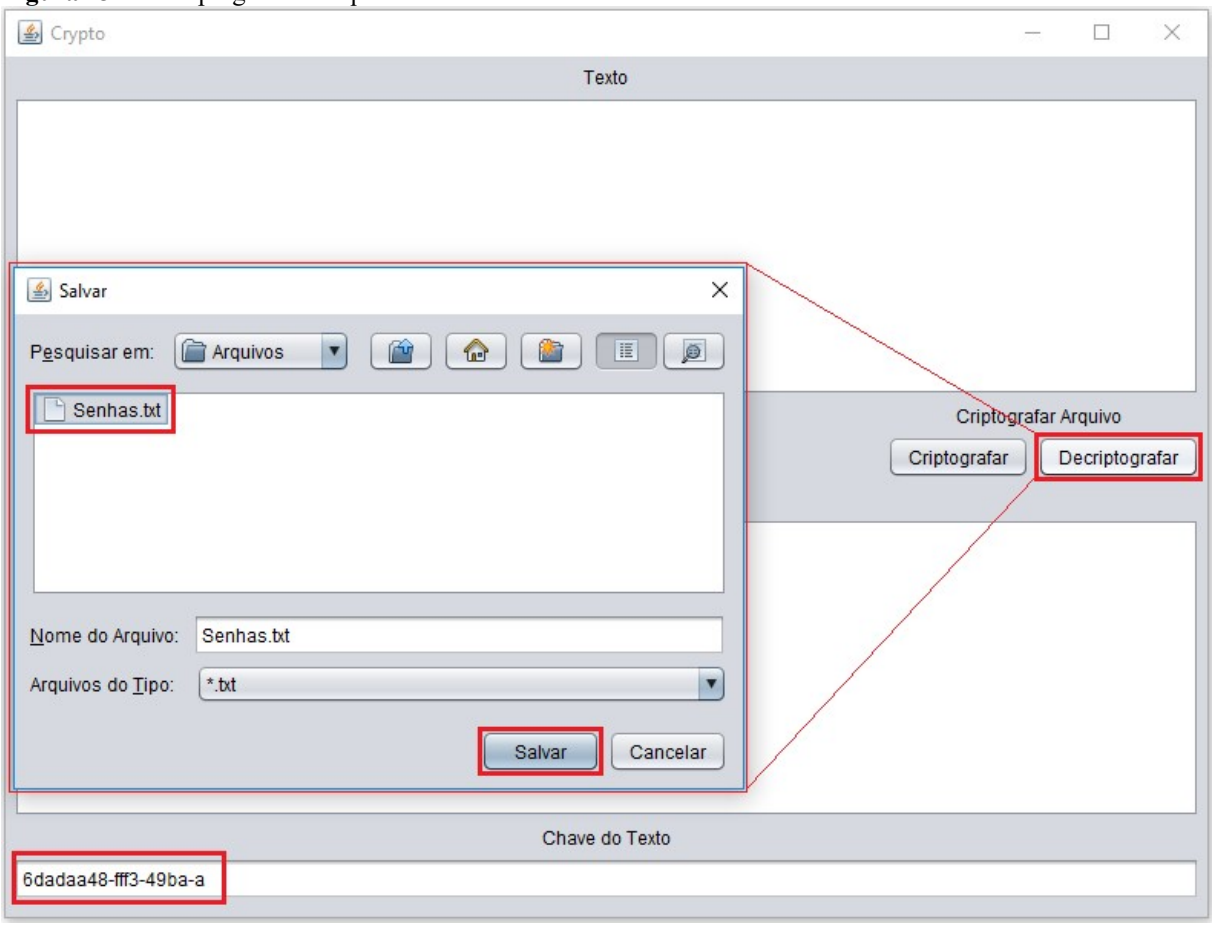
Figura 12 – Arquivo criptografado



Fonte: Elaborado pelo autor (2018).

Do mesmo modo que, era indispensável ter texto criptografado e chave no método anterior, neste, novamente, serão ambos indispensáveis. Contudo, agora clicando no botão "**Decriptografar,** " da operação "**Criptografar Arquivo,** " e selecionando o arquivo que foi criptografado simultaneamente com a senha, o conteúdo do arquivo será revertido ao seu texto original (Figura 13).

Figura 13 – Decriptografar o arquivo



Fonte: Elaborado pelo autor (2018).

A partir dos resultados obtidos, foi possível verificar que a metodologia de criptografia simétrica utilizada neste trabalho garante o sigilo das informações. Corroborando com os resultados alcançados, Paccamicio (2015) concluiu que o uso de um aplicativo para criptografar arquivos é eficiente para garantir a proteção de informações sigilosas pessoais, contra terceiros não autorizados. Fazendo o uso da criptografia simétrica, é possível proteger as informações de uma maneira mais confiável e robusta, uma vez que, somente a pessoa em posse da senha será capaz de reverter o processo e acessar o arquivo.

Em um trabalho elaborado por Santos e Souza (2015), os autores afirmam que os algoritmos simétricos são mais indicados para mensagens com grande volume de dados,

devido ao desempenho na execução, enquanto os assimétricos ficariam a cargo dos cenários em que se desconsideraria o uso de canais seguros para o compartilhamento de chaves.

Já Andrade (2012) utilizando o método de criptografia assimétrica, implementou um algoritmo baseado na linguagem C, buscando segurança e desempenho na execução da criptografia. Os resultados obtidos por ele demonstram que a escolha do tamanho da chave influencia diretamente na segurança e na velocidade da execução, visto que, com chaves menores, a segurança é menor. No entanto, a velocidade é elevada e com chaves maiores se prioriza a segurança em detrimento da velocidade.

Apesar dos autores Santos e Souza (2015) e Andrade (2012) evidenciarem que o modelo simétrico é mais rápido, concluo que em grandes volumes de dados, o *software Crypto* apresentou lentidão, não devido ao modelo simétrico e nem ao tamanho da chave, mas sim devido ao modelo de criptografia desenvolvido.

Comparando os resultados encontrados neste artigo com os autores mencionados acima, destaca-se, que a aplicação desenvolvida neste trabalho, apesar de utilizar a ideia de criptografia simétrica, não utiliza modelos de criptografia já existentes, mas sim desenvolve um novo modelo, baseado em métodos já existentes.

5 CONSIDERAÇÕES FINAIS

Em geral, foi possível verificar que, apesar do tema abordado não se constituir como assunto novo, foi capaz de alcançar o objetivo do artigo, aprofundando o conhecimento sobre o tema proposto.

Além disso, os resultados obtidos mostram o quão importante é a criptografia, enfatizando ainda mais a necessidade e eficiência da proteção de informações pessoais e corporativas, haja vista que, ao mesmo tempo em que os métodos de criptografia se aperfeiçoam, existem pessoas dispostas e interessadas em criar novas maneiras de quebrar a barreira da privacidade das informações sigilosas.

Portanto, ainda que a criptografia seja capaz de prover um ambiente seguro, não deve ser encarada como a solução definitiva e exclusiva em segurança, devendo trabalhar em conjunto com outras tecnologias. O *Crypto* apresentou lentidão no processamento de grandes volumes de dados, mas não por utilizar o método simétrico ou muito menos pelo tamanho de sua chave, mas sim pelo modo de desenvolvimento da criptografia. A evolução dessa aplicação não cessará com o fim deste trabalho, seguindo com o objetivo de construir um *software* cada vez mais seguro e que consiga suportar diferentes tipos de arquivos.

REFERÊNCIAS

ANDRADE, R. S. Algoritmo de criptografia RSA: Análise entre segurança e velocidade. **Revista Eventos Pedagógicos.** Sinop, v. 03, p. 438-457, dez. 2012

BRAZIL, G. W. **Protegendo redes ad hoc com certificados digitais e limite criptográfico.** 2007. 14 f. Dissertação (Mestrado em Computação) - Universidade Federal Fluminense, Niterói.

CASTRO, F. L. **Criptografia RSA:** uma abordagem para professores do ensino básico. 2014. 61 f. Trabalho de Conclusão de Curso (Licenciado em Matemática) – Universidade Federal do Rio Grande do Sul.

CHEUNG Y. H. O. ***Implementation of an FPGA Based Accelerator for Virtual Private Networks.*** 2002. 84 f. Dissertação de Mestrado **(**Mestre em Filosofia, Ciência da Computação e Engenharia**) -** The Chinese University of Hong Kong, Hong Kong.

COUTINHO, S. C. **Criptografia.** Rio de Janeiro: IMPA, 2008.

DIFFIE, W; HELLMAN, M. E. *New Directions in Cryptography.* ***Ieee transactions on information theory.*** New York, v.22, p.644-654, 1976.

FARIA, F. O. **Estudo da técnica de Criptografia Algoritmo Posicional – Alpos na segurança de dados de um banco de dados.** 2006. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdades Santo Agostinho.

FLICK, U. **Introdução à Pesquisa Qualitativa.** 3. ed. São Paulo: Artmed, 2009.

KAHN, D. ***The codebreakers: The story of Secret Writing.*** New York: Scribnet, 1996.

KÖCHE, J. C. **Fundamentos de Metodologia Científica:** Teoria da ciência e iniciação à pesquisa. Petrópolis: Vozes, 2011.

MACÊDO, D. **Chaves simétricas e assimétricas.** 2011. Disponível em: <https://www.diegomacedo.com.br/chaves-simetricas-assimetricas/> Acesso em: 05 Set 2018.

MARCACINI, A. T. R. **Direito e Informática:** uma abordagem jurídica sobre a criptografia. São Paulo: Forence, 2010.

NAKAMURA, E. T.; GEUS, P.L. Segurança de Redes em Ambientes Cooperativos. *In* NAKAMURA, E. T.; GEUS, P.L. **A criptografia e a PKI**. São Paulo: Novatec, p. 301-330, 2007.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. **Revista Segurança Digital.** [on-line], v. 05, p. 11-15, mar. 2012; continuação: v. 06, p. 21-24, mai. 2012.

PACCAMICIO, I. B. **Aplicativo de criptografia simétrica ACEcrypt.** 2015. 84 f. Trabalho de Conclusão de Curso (Tecnólogo em Segurança da Informação) – Faculdades Integradas Promove de Brasília.

SANTOS, D. A.; SOUZA, R. R. **Estudo sobre o desenvolvimento de aplicações VOIP para plataforma Windows com criptografia.** 2015. 59 f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Universidade Federal do Estado do Rio de Janeiro.

SETESYS, Produtividade Corporativa. **Como produzir senhas criativas utilizando a Cifra de César.** 2016. Disponível em: <http://setesys.com.br/blog/como-produzir-senhas-criativas-utilizando-a-cifra-de-cesar/> Acesso em: 05 de Set. 2018.

SILVA, E. V. P. **Introdução à Criptografia RSA.** 2006. 29 f. Trabalho de Conclusão de Curso (Licenciado em Matemática) – Universidade Estadual Paulista Júlio Mesquita Filho.

SINGH. S. **O livro dos códigos.** Rio de Janeiro: Record, 2008.

STALLINGS. W. **Criptografia e segurança de redes:** Princípios e práticas. São Paulo: Pearson Prentice Hall, 2008.

VOITECHEN, D. A. **Análise e Comparação de Algoritmos Para Criptografia de Imagens.** 2015. 159 f. Trabalho de Conclusão de Curso (Tecnóloga em Análise e Desenvolvimento de Sistemas) - Universidade Tecnológica Federal do Paraná.

WYKES, S. M. **Criptografia Essencial:** a jornada do criptógrafo. Rio de Janeiro: Elsevier, 2016.

ZOCHIO, M. F. **Introdução à Criptografia.** São Paulo: Novatec, 2016.