Criptografia RSA e de Ponta a Ponta

Gabriel D. Silva[1], Osnel Broche Cristo [2]
PROFMAT UFLA, Lavras, MG
Universidade Federal de Lavras, Lavras, MG

Resumo. Em meio aos avanços tecnológicos, cada vez se torna mais necessário a garantia da integridade de uma informação ou troca de dados. Para garantir a segurança, utiliza-se a criptografia, tal método já passou por diversas modificações, inicialmente conhecida com Cifra de César, utilizada por César para garantir a integridade da mensagem enviada, consiste apenas na troca de letras respeitando uma lei de formação, que pode ser definida por uma função afim. Com os avanços nas comunicações, esse método foi ficando falho, exigindo modificações e criações de novos métodos de criptografia, chegando assim na criptografia RSA (Rivest-Shamir-Adleman), atualmente utilizada nos mais diversos tipos de criptografia.

A criptografia RSA utiliza o método assimétrico, que consiste em duas etapas, ou seja, o par de chaves utilizadas para criptografar e descriptografar são diferentes, conhecidas como chave pública e chave privada respectivamente, sendo que apenas o receptor da mensagem possui a chave privada para descriptografar a mesma. Para a funcionalidade do RSA precisa-se de um número n que é o produto de dois primos distintos, utilizado para codificar e quanto maiores forem os números primos, maior será a dificuldade de se quebrar a mensagem criptografada. Para conseguir gerar os pares de chaves públicas e privadas no sistema RSA é necessário encontrar o valor da função Phi de Euler (ϕ) de n, pois a chave pública é formada pelos números (e, n), tal que e é invertível módulo $\phi(n)$ e a chave privada é formada por (d, n) tal que d é o inverso de e módulo $\phi(n)$.

As comunicações realizadas pelo WhatsApp estão protegidas pela criptografia de ponta a ponta, que garante uma maior segurança nas trocas de informações, pois apenas as pessoas que estão se comunicando por meio dos aparelhos que são capazes de compreender e armazenar as mensagens. O método utilizado é o RSA, neste caso existem 4 pares de chaves, sendo os pares de chaves públicas e privadas do remetente e os pares de chaves públicas e privadas do destinatário.

Palavras-chave. RSA, Criptografia de Ponta a Ponta.

1 Introdução

A palavra criptografia traduzida para o Grego é composta por duas partes, "cryptos"que significa oculto, e "graphos"que significa escrever. Desta forma podemos dizer que a criptografia vista como a "arte de codificar"faz parte de um grupo de conhecimentos e técnicas, que produzem mensagens codificadas, que só podem ser decodificadas através de chaves[6], garantindo assim que apenas quem envia e quem recebe a informação consegue compreender o que está sendo compartilhada, desta forma, produzindo uma segurança nas trocas das informações.

Um dos primeiros métodos de criptografia, é o método de César, que consiste em trocar a sequência das letras da informação original, por uma sequência de letras que respeitem a lei de

[1]gabriel.silva59@estudante.ufla.br
[2]osnel@ufla.br

formação, seguindo assim um determinado padrão na codificação, podendo ser relacionada com a função afim

$$f(x) = x + b \tag{1}$$

sendo x a variável representando da letra de entrada e b o valor do qual acrescentará a substituição pela letra criptografada.

Inicialmente trabalhava-se apenas com a possibilidade da criptografia *simétrica*, onde a mesma consiste que a chave utilizada na codificação da mensagem, era a mesma utilizada para decodificar. Porém com os avanços tecnológicos, surgiu o problema de compartilhar a chave de forma segura sem que a mesma seja interceptada por outros, este fato deu origem então a criptografia *assimétrica* que consiste em duas chaves diferentes, a chave pública e a chave privada, tornando assim uma dificuldade maior para decodificar uma mensagem caso a mesma fosse extraviada. A chave pública é utilizada para a codificação da mensagem, e apenas quem possui a chave privada é capaz de decodificar essa mensagem. Veremos agora algumas diferenças e vantagens dos dois sistemas.

A criptografia simétrica possui as seguintes vantagens: a mesma chave utilizada para criptografar uma mensagem é a mesma utilizada para descriptografar, não depende tanto de recursos tecnológicos, é de fácil utilização e interpretação e o texto criptografado é menor ou do mesmo tamanho que o texto original. Este formato é mais indicado quando exige uma rapidez no envio da mensagem e não demanda um nível tão alto de segurança.

A criptografia assimétrica possui as seguintes vantagens: a chave privada não precisa ser compartilhada; garantindo assim um nível maior de segurança, é possível provar a autoria da mensagem por meios de assinaturas digitais., atinge um número maior de usuários já que cada um necessita apenas de um par de chaves, utilização elevada de recursos tecnológicos, um nível maior de complexibilidade para compreender, já o texto cifrado é do mesmo tamanho ou maior que o texto original, esse sistema também pode ser utilizado para assinaturas digitais, garantindo assim a integridade e autenticidade da mensagem.

O WhatsApp [2] protege as conversas por uma criptografia conhecida como ponta a ponta, tal processo é realizado pela composição de 4 chaves, sendo um par de chave pública e privada do remetente e outro par de chaves do receptor.

2 Metodologia

A pesquisa é uma sequência de etapas estipulada pelo pesquisador. A pesquisa como sendo a inquisição, o procedimento sistemático e intensivo, que tem por objetivo descobrir e interpretar os fatos que estão inseridos em uma determinada realidade. Fachin [4] destaca que a pesquisa é, “um procedimento intelectual para adquirir conhecimentos pela investigação de uma realidade e busca de novas verdades sobre um fato”.

Já para definirem-se os caminhos da pesquisa, é necessário classificá-la. Quanto à natureza está pesquisa é básica, pois possui a finalidade de explicar a segurança nos meios de comunicação especialmente no WhatsApp. Para Gil [5] "a pesquisa básica aglutina estudos que têm como objetivo completar uma lacuna no conhecimento". Isso nos remete a Schwartzman [7] que descreve que a pesquisa básica é "aquela que acumula conhecimentos e informações que podem eventualmente levar a resultados acadêmicos ou aplicados importantes, mas sem fazê-lo diretamente".

Quanto aos objetivos, a classificação metodológica desta pesquisa é a descritiva, pois deste estudo pretende descrever os fatos e fenômenos de determinada realidade.

Em relação à abordagem, esta pesquisa é qualitativa. Para Minayo [8]"a pesquisa qualitativa trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis". Também, nesta mesma linha, Denzin e Lincoln [3] pontuam que, "a pesquisa qualitativa é uma atividade situada que localiza o observador em

um conjunto de práticas matérias e interpretativas que dão visibilidade ao mundo em uma série de representações". Busca-se entender o fenômeno em termo dos significados que as pessoas a ele conferem.

Já o procedimento metodológico adotado é a pesquisa bibliográfica, que consiste basear-se em obras publicadas para explicar o problema.

3 Desenvolvimento

A criptografia RSA [1] utiliza o método assimétrico, que consiste em duas etapas, sendo o par de chaves utilizadas para criptografar e descriptografar diferentes, conhecidas como chave pública e chave privada. Apenas o receptor da informação possui a chave privada que é capaz de descriptografar a mesma. Para a funcionalidade do RSA, precisa-se de um número n que é o produto de dois primos distintos e quanto maiores forem os números primos, maior será a dificuldade de se quebrar o códico da mensagem criptografada. Para conseguir gerar os pares de chave pública e privada, no sistema RSA é preciso encontrar o valor da função Phi de Euler (ϕ) de n, pois a chave pública é formada pelos números (e, n), tal que e é invertível módulo $\phi(n)$ e a chave privada é formada por (d, n) tal que d é o inverso de e módulo $\phi(n)$.

A criptografia de ponta a ponta utilizada pelo WhatsApp garante uma segurança maior nas informações, pois apenas as pessoas que possuem os aparelhos que estão se comunicando possuem acesso às informações trocadas e são capazes de armazenar as mesmas; sendo a composição dos pares de chaves o formato RSA. Supondo uma comunicação entre Alice e Bob com as chaves públicas e privadas respectivamente de Alice $(e, n), (d, n)$ e as respectivas chaves de Bob (e_1, n) e (d_1, n), a função que criptografa a mensagem enviada de Bob para Alice é $f_a(x)$ e a função utilizada por Alice para descriptografar a mensagem recebida é $f_a^{-1}(x)$ e a função que criptografa a mensagem enviada de Alice para Bob é $g_b(x)$ e a função utilizada por Bob para descriptografar a mensagem recebida é $g_b^{-1}(x)$. Alice vai enviar para Bob uma mensagem X então a mensagem que vai estar navegando na internet será: $g_b(X) = Y$ assim a mensagem que chega a Bob é Y para descriptografar Bob realiza o seguinte processo: $g_b^{-1}(Y) = X$ de modo análogo se Bob decide enviar uma mensagem X para Alice temos : $f_a(X) = Y$ e $f_a^{-1}(Y) = X$ para criptografar e descriptografar respectivamente.

O WhatsApp possui a opção para realização de pagamentos e pedido de pagamento, para isso utiliza a composição de funções entre as pontas da conversa, para que esta opção seja realizada primeiro é utilizada a chave privada do emissor, logo após a chave pública do receptor, assim a comunicação de transferência está passando por duas criptografia, desta forma quando o comunicado de pagamento chegar ao seu destino o processo para descriptografar é da seguinte maneira: primeiro utiliza a chave privada do receptor, logo após a chave pública do emissor, assim a mensagem navega por um sistema de redes com um maior nível de segurança.

Em uma transferência entre Alice e Bob, pelo WhatsApp sendo as chaves públicas e privadas respectivamente de Alice $(e, n), (d, n)$ e as respectivas chaves de Bob (e_1, n) e (d_1, n). Considere a função $f_a(x)$ como criptografar o pagamento com a chave pública de Alice e a função inversa $f_a^{-1}(x)$ como descriptografar utilizando a chave privada de Alice, e $g_b(x)$ como criptografar com a chave pública de Bob e $g_b^{-1}(x)$ como descriptografar utilizando a chave privada de Bob. Supondo que Alice vai realizar um pagamento X para Bob. A informação Y que está sendo compartilhada é criptografada pelo sistema de ponta a ponta, dada pela seguinte imagem da função composta:

$$g_b(f_a^{-1}(X)) = Y \tag{2}$$

para Bob descriptografar a informação Y, Bob realiza o seguinte processo também de compo-

sição de funções usando as distintas chaves:

$$f_a(g_b^{-1}(Y)) = X \tag{3}$$

Desta forma apenas Alice e Bob possuem acesso às informações compartilhadas. De modo análogo para informações compartilhadas de Bob para Alice, temos o seguinte esquema:

$$\begin{aligned} \mathrm{f}_a(g_b^{-1}(X)) &= Y \\ \mathrm{g}_b(f_a^{-1}(Y)) &= X \end{aligned} \tag{4}$$

4 Considerações Finais

Durante todo processo de evolução das comunicações, existiu a necessidade da segurança do envio de, informações, garantindo a integridade das mesmas.

Com as reformas no novo ensino médio, a integração de disciplinas com o uso de computadores, a interdisciplinalidade com matérias voltadas para o uso computacional e a matemática.

Com a parte matemática utilizando as funções inversas e composição de funções é possivel explicar e mostrar como funciona a criptografia, como é realizado o processo de segurança das comunicações em redes inseguras, com o auxilio computacional mostrar na prática o processo de criptografia. [9].

Para que uma conversa, ou até mesmo uma negociação no formato digital é necessário garantir a privacidade do conteúdo compartilhado entre as pessoas na comunicação virtual, tal segurança é obtida com a criptografia, que pode ser composta por uma ou mais funções, relacionando de acordo com a necessidade e o nível de segurança desejado.

O meio de comunicação que se tornou mais popular nos últimos anos foi o WhatsApp, que utiliza a criptografia de ponta a ponta garantindo um nível de segurança mais elevado comparado com os demais formatos, sendo assim o meio utilizado pelo WhatsApp garante a integridade e segurança de seus usuários, além do mais apenas as pessoas que possuem os aparelhos que estão realizando as comunicações são capaz de armazenar as informações, apenas deve se tomar cuidado com a realização do backup, pois o lugar que for realizado o mesmo pode ser de segurança baixa, perdendo assim a confiabilidade dos arquivos.

Referências

[1] STEVEN BURNETT. **Criptografia e segurança: o guia oficial RSA**. Gulf Professional Publishing, 2002.

[2] Camila Giacometti Colasuonno. "A implantação da criptografia do whatsapp e a obrigação de fornecimento de dados pelo facebook". Em: (2022).

[3] Norman K Denzin e Yvonna S Lincoln. **O planejamento da pesquisa qualitativa: teorias e abordagens**. Artmed, 2006.

[4] Odília Fachin. "Fundamentos de metodologia". Em: **Fundamentos de metodologia**. 2003, pp. 200–200.

[5] Antônio Carlos Gil. **Como elaborar projetos de pesquisa**. Editora Atlas SA, 2002.

[6] Alexandre Menezes Ribeiro, Evandro Luiz de Oliveira, Pedro Pinheiro Cardoso e Viviane Regina Lemos Bertol. "A Infra-estrutura de Chaves Públicas Brasileira e suas bases para a Auditoria em Segurança da Informação". Em: **Brasília (DF), Novembro de** (2004).

[7] Simon Schwartzman. “Pesquisa acadêmica, pesquisa básica e pesquisa aplicada em duas comunidades científicas”. Em: **Termos de referência de pesquisa, não publicado, janeiro de** (1979).

[8] Maria Cecília de Souza Minayo, Suely Ferreira Deslandes e Romeu Gomes. **Pesquisa social: teoria, método e criatividade**. Editora Vozes Limitada, 2011.

[9] Idemar Vizolli, Euvaldo Euvaldo de Souza Carvalho e Onésimo Rodrigues Pereira. “CRIPTOGRAFIA: UMA POSSIBILIDADE PARA O ENSINO DE FUNÇÃO INVERSA”. Em: **REAMEC-Rede Amazônica de Educação em Ciências e Matemática** 7.1 (2019), pp. 196–212.