Criptografia RSA nas comunicações

Gabriel Davi da Silva[1], **Osnel Broche Cristo** [1]

1-Departamento de Matemática e Matemática Aplicada/ICET – Universidade Federal de Lavras (UFLA) Caixa Postal 3037 – 37203-202 – Lavras, MG – Brasil

gabriel.silva59@estudante.ufla.br, osnel@ufla.br

Palavras-chave: Criptografia de Ponta a Ponta, RSA

Em meio aos avanços tecnológicos, cada vez se torna mais necessária a garantia da integridade de uma informação. 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 o passar dos tempos esse método foi ficando falho, exigindo modificações e criações de novos métodos de criptografia, chegando assim, à criptografia RSA (Rivest-Shamir-Adleman), atualmente utilizada nos mais diversos tipos de criptografia.

A criptografia RSA utiliza o método assimétrico, as chaves utilizadas para criptografar e descriptografar são diferentes, conhecidas como chaves pública e privada, respectivamente. Apenas o receptor da mensagem possui a chave privada para descriptografar a mensagem. 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 a mensagem criptografada. Para conseguir gerar o par de chaves no sistema RSA é necessário encontrar o valor da função Phi de Euler (φ) de n, pois a chave púbica é formada pelos números (e, n), tal que e é invertível módulo $\varphi(n)$ e a chave privada é formada por (d, n), tal que d é o inverso de e módulo $\varphi(n)$.

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 possuem os aparelhos que estão se comunicando são capazes de compreender e armazenar as mensagens. O método utilizado é o RSA, neste caso existem quatro pares de chaves, sendo os pares de chave pública e privada do remetente e os pares de chave pública e privada do destinatário.

Neste trabalho será apresentado a funcionalidade do RSA, porque a criptografia de Ponta a Ponta garante um nível de segurança maior que outros métodos de criptografia, e como é realizado a segurança nas trocas, de informações e de pagamentos no WhatsApp.