Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Criptografia RSA e Algoritmo de Shor: Entendendo o Problema.

Raissa Karoliny Da S. Rodrigues[1]
CCT - Universidade Federal do Cariri
Clarice Dias de Albuquerque[2]
CCT - Universidade Federal do Cariri

A técnica de criptografar é conhecida e utilizada há milhares de anos. Ao longo do tempo, muitos métodos para ocultar informações tornaram-se menos viáveis devido à facilidade de decifrá-los. Todavia, com o avanço da tecnologia a criptografia tornou-se mais eficaz e segura, além de indispensável diante da necessidade de proteger dados pessoais, senhas e qualquer outra informação compartilhada na internet.

Embasado na teoria dos números, o método RSA, criado em 1977, foi o primeiro modelo de criptografia de chave pública [1], amplamente utilizado por sua segurança. Porém, com o surgimento do algoritmo de Shor publicado em 1994 [2], a segurança do método RSA foi posta em risco e desde então muitos estudos estão direcionados para modelos criptográficos resistentes a possíveis ataques quânticos.

A segurança do método RSA baseia-se na dificuldade de se encontrar os fatores primos de um número n muito grande. A partir dos fatores primos p e q de n, determinam-se $\phi(n)$ e as chaves pública e privada e e d, respectivamente.

Para demonstrar o funcionamento do método, iremos ilustrar através de um exemplo com números pequenos. Tome $p = 3$ e $q = 11$, então $n = p \times q = 33$. O par de chaves públicas (n, e) precisa do valor de $\phi(n)$ para encontrar e, um número inteiro positivo inversível módulo $\phi(n)$, ou melhor, $\text{mdc}(e, \phi(n)) = 1$

$$\phi(n) = (p-1) \times (q-1) \tag{1}$$

Para o par de chaves privadas (n, d), d deve ser um número tal que seja o inverso de e em $\phi(n)$,

$$d \times e \equiv 1 \ (\text{mod } \phi(n)). \tag{2}$$

neste caso $e = 7$ e $d = 3$. Assim, a chave privada é $(33, 3)$, e a pública $(33, 7)$. Com todos os valores calculados iremos encriptar uma mensagem para ilustrar o método, supondo que a letra R corresponda ao número 16 em uma dada tabela e d seja o bloco a ser codificado, $d = 16^7 \bmod 33$, encontrando $d = 25$ que é a mensagem codificada. Para o processo inverso, ou seja, a decodificação, seja c o bloco decodificado, então $c = 25^3 \bmod 33$, $c = 16$.

Em contrapartida, o algoritmo de Shor usa propriedades da mecânica quântica para encontrar os fatores primos de um número N. Para isso busca-se um número x coprimo com N, tal que $1 < x < N$. O objetivo é encontrar a ordem r de x, de modo que r não pode ser impar e $(x^{r/2} - 1)$ e $(x^{r/2} + 1)$ não podem ser múltiplos de N.

$$x^r \equiv 1 \bmod N \tag{3}$$

[1]raissateixeir4@gmail.com
[2]clarice.albuquerque@ufca.edu.br

O computador quântico começa no estado $|\psi_0\rangle = |0\rangle|0\rangle$, o primeiro registrador possui t qubits, dado que $N^2 \leq 2^t \leq 2N^2$ e o segundo n qubits, sendo $n = \lceil \log_2 N \rceil$. O primeiro passo é a aplicação da porta de Hadamard sobre os qubits do primeiro registrador, deixando-os em uma superposição de todos os estados da base computacional com igual amplitude dada por $\frac{1}{\sqrt{2^t}}$, [3], depois é aplicado um operador linear unitário V_x donde $V_x(|j\rangle|k\rangle) = |j\rangle|k + x^j\rangle$, tal que $|j\rangle$ e $|k\rangle$ são respectivamente os estados do primeiro e do segundo registrador. V_x gera todas as potências de x de maneira simultânea e é feita uma medida no segundo registrador, gerando números com igual probabilidade. O último passo é a aplicação da Transformada de Fourier Inversa $DFT^{-1} = DFT^{\dagger}$, no primeiro registrador, pois o período do estado do primeiro registrador é a solução para o problema, e a transformada de Fourier pode revelar o valor deste período,[2]. Assim, para $N = 21$ e $x = 2$, temos $t = 9$ e $n = 5$, aplicando o algoritmo de Shor esperamos encontrar $r = 6$. Logo, $\text{mdc}(x^{r/2} - 1, N)$ e $\text{mdc}(x^{r/2} + 1, N)$, nos dará os fatores 7 e 3.

Sob essa perspectiva concluímos que o método RSA permanece seguro contra ataques de algoritmos clássicos, que não conseguem obter os fatores primos p e q de um dado n consideravelmente grande, no entanto, com o surgimento de computadores quânticos, que podem realizar vários cálculos em paralelo [4], e algoritmos como o de Shor, o RSA pode eventualmente deixar de ser seguro. Logo a pesquisa em torno de métodos criptográficos mais robustos, visando assegurar a proteção eficaz das comunicações e informações suscetíveis a ataques quânticos, faz-se cada vez mais necessária.

Agradecimentos

Agradeço a Universidade Federal do Cariri (UFCA), que possibilitou essa pesquisa por meio da bolsa de iniciação científica e da estrutura física.

Referências

[1] A. C. Faleiros. **Criptografia**. Vol. 52. Notas em Matemática Aplicada. São Carlos, SP: SBMAC, 2011. ISBN: 978-85-86883-54-5.

[2] R. Portugal, C. C. Lavor, L. M. Carvalho e N. Maculan. **Uma Introdução à Computação Quântica**. 2a. ed. Vol. 8. Notas em Matemática Aplicada. São Carlos, SP: SBMAC, 2012. ISBN: 978-85-86883-61-3.

[3] L. A. Vieira e C. D. Albuquerque. "Um estudo passo a passo dos algoritmos de Grover e Shor". Em: **Revista Eletrônica Paulista de Matemática** 19 (2020), pp. 1–20. DOI: 10.21167/cqdvol19ic2010231696641avcda0120.

[4] S. R. Fernandes, J. T. Assis, G. Carvalho e V. V. Estrela. "Criptografia Quântica, Uma Abordagem Introdutória". Em: **Proceedings do X Encontro de Modelagem Computacional**. Vol. 1. Nova Friburgo: ABCM, 2007, pp. 1–9.