Criptografia: da história até a aplicação do método RSA.

Tauana Bianchetti[1]
Caroline Saúgo[2]
Neuza Terezinha Oro[3]

Resumo

A palavra criptografia vem do grego “Cryptos” e significa “secreto, oculto”. É a arte do código secreto e se desenvolveu devido ao avanço das tecnologias. Criptografia é a Ciência que estuda princípios e técnicas para escrever uma mensagem em código, de modo que uma mensagem escrita com clareza para o destinatário se torne incompreensível para outras pessoas. Neste contexto, é muito importante conhecermos a evolução de processos de criptografar mensagens, pois este vem sendo utilizado há muitos anos, sobretudo em assuntos ligados à guerra, ao amor, à diplomacia e, atualmente, à segurança de senhas e dados computacionais.

Para realizamos a pesquisa sobre a história, inicialmente fizemos um levantamento de bibliografias quanto à história da criptografia. Dividimos em épocas, de acordo com o desenvolvimento histórico, classificando em criptografia clássica e moderna. Onde na criptografia clássica, vimos que o primeiro código secreto investigado e que se teve notícias foi o Código de César, que não se mostrou muito eficiente por ser fácil de quebrar. Em seguida, surge uma nova maneira na qual se torna inviável a aplicação de uma contagem por frequência. Para, a mensagem é subdividida em blocos de várias letras e estes blocos são embaralhados, esse processo de criptografar mensagem é conhecido como Código de Blocos. Este processo embora, tenha se mostrado mais eficiente que o primeiro, não foi muito aprovado, pois também não garante total segurança. A seguir, passamos a investigar a criptografia moderna, que está alicerçada aos Códigos de Chave Pública, onde o método mais conhecido e utilizado é o chamado RSA. O método de criptografia de chave pública RSA, sigla de seus criadores Ron Rivest, Adi Shamir e Len Adelmam.

Para codificarmos uma mensagem, no RSA, precisamos de alguns conhecimentos matemáticos, como a teoria dos números. Foram estudados vários métodos de codificação: códigos formados por meio de permutações das letras e os procedimentos usados no método RSA, onde converte-se uma mensagem a uma sequência de números, mas a mensagem deve ter apenas letras. A seguir foi escolhida

[1] Acadêmica do Curso de Matemática na Universidade de Passo Fundo; 102118@upf.br
[2] Acadêmica do Curso de Matemática na Universidade de Passo Fundo; 98516@upf.br
[3] Professora do Curso de Matemática na Universidade de Passo Fundo; neuza@upf.br

uma palavra, substituída por número e utilizado o método de criptografia RSA. A princípio definimos dois números primos p e q e depois calculamos o seu produto n. Na próxima fase, precisamos quebrar em blocos o número que representa a mensagem, porém os números dos blocos não devem ser maiores que n e nem começarem com zero. O número n é chamado de chave pública. Escolhendo os dois números primos e resolvendo o seu produto ,devemos encontrar por meio da fórmula (n)= (p-1)(q-1).Por fim escolhemos e, que deve ser o menor primo que não divide o. Assim, cada bloco é codificado como o resto da divisão deste número elevado em e por n.

Para decodificar uma mensagem, no RSA, também foram necessários estudos sobre números primos e aritmética modular. Após, fez-se uma investigação sobre os passos da decodificação pelo método RSA, descritos a seguir. Quando o receptor recebe a mensagem codificada, é conhecida a chave pública, que é obtida através do produto de p e q (números primos). Com esta chave, precisamos obter o inverso do menor primo e que não divide a função definida pelo produto de (p-1).(q-1). Isto é realizado através da obtenção do resto da divisão da função produto pelo número e. Considerando que não conhecemos os números primos p e q, que geralmente são muito grandes e que o produto deles é um número maior ainda e representa a chave pública no método RSA, fica difícil a fatoração manual deste número. Então, neste passo, utilizamos o *software maple* para obter o inverso do número e. Desta forma, realizarmos a decodificação, ou seja, a obtenção da mensagem inicial.

Neste contexto, este resumo apresenta a proposta metodológica da oficina "Criptografia: da história até a aplicação do método RSA", na qual destacamos a evolução histórica da criptografia e os princípios matemáticos para codificar e decodificar mensagens através do método RSA, enfatizando a importância da teoria dos números para aplicação da matemática como agente motivador de seu ensino em sala de aula.

Palavras-chave: Criptografia; História; Codificar e decodificar mensagens; Teoria dos números;

Referências

COUTINHO, S. C. Criptografia. Programa de Iniciação Científica da OBMEP 2007, n. 7.Rio de Janeiro: Imprinta Express Gráfica e Editora Ltda, 2007.

COUTINHO, S. C. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA, 2009.