
Atividades de Contagem a partir da Criptografia

LOPES, Heitor Curado Maciel

Instituto Federal de Goiás, Câmpus Formosa.

SANTOS, Laredo Rennan Pereira

Instituto Federal de Goiás, Câmpus Formosa.

Este projeto visou o estudo de atividades de contagem que surgem a partir de sistemas de codificação de mensagens. A codificação de informações está presente em muitas tarefas essenciais do dia a dia, como aquelas que envolvem transações financeiras e o uso seguro da Internet, ou mesmo em situações que não envolvem o sigilo de dados, tal como a codificação de sinais para formar a Escrita Braille. Nosso objetivo foi apresentar atividades com criptografia através de aparatos que possam efetivamente ser construídos com materiais simples (papel, palito de dente, clipe, furador de papel, cola e tesoura) para explorar alguns aspectos matemáticos destas construções, principalmente os ligados à contagem. Uma dessas construções feitas foi o Quadro de Viginère, o qual é uma tabela que fornece todas as maneiras de rearranjo das letras do alfabeto para uma codificação usando a cifra de César. Consideramos também problemas de contagem associados à Escrita Braille. Este é um sistema baseado em um arranjo 3x2 de pontos, como nas pedras de um dominó. Uma questão interessante seria considerar quantas configurações possíveis podem ser obtidas pela Escrita Braille. Esta questão é facilmente respondida usando o Princípio Multiplicativo da Contagem, mas abordamos o problema de diversas maneiras: Quantas seriam as configurações possíveis, marcando apenas três pontos? Se quisermos codificar todas as letras minúsculas, maiúsculas, os algarismos de 0 a 9, os sinais de pontuação (ponto final,

dois pontos, ponto de interrogação, ponto de exclamação e vírgula) e os quatro sinais de operações matemáticas, os padrões obtidos nas dimensões 3×2 serão suficientes? Em um sistema de escrita com uma célula $n \times m$, quantas configurações diferentes podemos formar? Para responder a essas questões recorreremos ao conceito de Combinação Matemática. Outro sistema muito semelhante ao usual da linguagem Braille 3×2 é o sistema em que as células possuem uma linha somente e seis colunas. Sistemas do tipo $1 \times n$ servem para escrever números na base 2 e, assim sendo, têm muitas aplicações na Matemática e na Informática. Podemos escrever qualquer número natural na base 2, utilizando-se para isto apenas os dígitos 0 e 1. Este modo de escrita é conhecido como Sistema Binário. Os números de 0 a 63 podem ser escritos na base 2 por meio de 6 dígitos. Dessa forma, há uma correspondência entre estes números escritos no Sistema Binário e sua representação no estilo Braille (o qual possui 64 configurações possíveis). Uma vez observado isto, concluímos que o Sistema Binário oferece uma nova forma de lidar com os problemas de contagem relacionados à linguagem Braille. Vê-se, assim, que o estudo de problemas de contagem relacionados à criptografia envolve muitos elementos importantes da Matemática, justificando a relevância da pesquisa.

Palavras-chave

Criptografia; Código Binário; Princípios de Contagem; Combinação Matemática.

Agradecimentos

O presente trabalho foi realizado com apoio do Instituto Federal de Goiás. Agradecemos ao CNPq pela bolsa concedida.