Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

O uso da Criptografia como ferramenta motivacional nas aulas de probabilidade no Ensino Médio

Willa da S. Medeiros[1]
EEEFM Antônio Gomes, PB
Maria Joseane F. G. Macêdo[2]
Jocivania Pinheiro[3]
de Ciências Exatas e Naturais, UFERSA, Mossoró, RN

A palavra criptografia deriva do grego *Kriptos* (secreto, oculto) e *graphein* (escrever). Como ciência, a Criptografia estuda e desenvolve métodos para tornar ilegível o conteúdo de uma mensagem, de maneira que apenas o receptor verdadeiro tenha condições de recuperar e ler seu conteúdo [3]. É notória a importância da Criptografia para a sociedade moderna. Suas aplicações evoluíram muito, e hoje é quase impossível pensar nossa vida sem a segurança que ela nos fornece. É importante destacar que a matemática foi a principal responsável por tal evolução, e que muitas noções simples de criptografia estão relacionadas com conceitos básicos de matemática do Ensino Médio. Para uma leitura mais aprofundada recomendamos [1].

Neste trabalho propomos abordar em sala de aula a relação entre probabilidade e criptografia através do conceito de Sigilo Perfeito, que é definido com base em probabilidade condicional através da seguinte ideia central: o indivíduo A desenvolve um método de criptografia para se comunicar com o indivíduo B e o intruso I pretende violar a comunicação entre A e B. Se A codifica o texto x e o manda para B, caso I tenha acesso ao texto codificado, o método utilizado por A e B será dito de sigilo perfeito se I não conseguir obter informação sobre x com base no texto cifrado em sua posse [1]. É extraordinário o fato de que esse problema pode ser modelado por meio da definição de probabilidade condicional com aplicações fora do contexto dos jogos de azar. Desse modo, o objetivo central é motivar, por meio da noção de sigilo perfeito, o estudo de probabilidade no Ensino Médio com a inclusão de exemplos e aplicações.

Pretende-se, por meio do problema de sigilo perfeito, falar de criptografia e de como os conceitos de probabilidade são importantes para estruturá-lo matematicamente. Utilizaremos exemplos simples de métodos criptográficos, onde nosso objetivo será mostrar que tal método possui sigilo perfeito.

Voltando ao problema do intercâmbio de mensagens de A e B, imaginemos que o intruso I consiga obter um dos textos cifrados c e seja P o espaço amostral dos textos comuns x. Supondo que I conhece a probabilidade definida pergunta-se: *qual é a probabilidade de x ter sido escolhido para codificação, sabendo que o texto cifrado correspondente é c*? Ou seja, I está procurando respostas sobre a probabilidade condicional de x dado c, denotada por $p(x|c)$. Para provar o sigilo perfeito do método em questão, utilizaremos a Proposição 1, que é uma releitura da apresentada em [1].

Proposição 1. *Sejam C o conjunto dos textos cifrados, K o conjunto das chaves utilizadas na codificação e $p(x)$ a probabilidade de x ser codificado. Considere um método criptográfico onde o*

[1]willamedeiros@hotmail.com
[2]joseane@ufersa.edu.br
[3]vaniamat@ufersa.edu.br

espaço de chaves é um espaço Amostral equiprovável, e os conjuntos C e K tem a mesma quantidade de elementos. Tal método será dito de sigilo perfeito se, e somente se, $p(x|c) = p(x)$.

O exemplo a seguir ilustra uma aplicação de tal proposição.

Exemplo 1. *Considere o criptossistema dado por $P = \{x, y\}$, $K = \{\alpha, \beta\}$ e $C = \{c_x, c_y\}$, com as seguintes probabilidades definidas. Em P: $p(\emptyset) = 0$, $p(P) = 1$, $p(x) = 3/5$ e $p(y) = 2/5$. Em K: $p(\emptyset) = 0$, $p(K) = 1$, $p(\alpha) = p(\beta) = 1/2$. Vamos verificar que este criptossistema possui sigilo perfeito.*

De fato, como a função de codificação é uma permutação, ela pode ser definida como $E_\alpha(x) = c_y$, $E_\alpha(y) = c_x$, $E_\beta(x) = c_x$ e $E_\beta(y) = c_y$. Então, escolhe-se um texto, uma chave e efetua-se a codificação. O diagrama de árvore a seguir mostra todas as possibilidades.

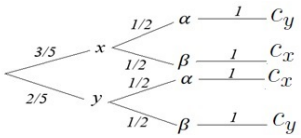

Figura 1: Diagrama de árvore para o problema.

Logo, $p(x|c_x) = \frac{p(x|c_x)}{p(c_x)} = \frac{\frac{3}{5}\cdot\frac{1}{2}}{\frac{3}{5}\cdot\frac{1}{2}+\frac{2}{5}\cdot\frac{1}{2}} = \frac{3}{5} = p(x)$. *Analogamente,* $p(y|c_y) = p(y)$.

Esperamos que tanto o aluno quanto o professor possam tirar proveito do uso da criptografia em sala de aula, e que essa abordagem diferenciada reflita na melhoria do ensino e na compreensão dos conceitos estudados. Ser capaz de compreender uma aplicação da matemática e enxergar a importância de determinado conceito pode ser a chave para despertar a curiosidade e o desejo em estudar essa ciência.

Agradecimentos

Os autores agradecem o apoio da UFERSA e do CNPq na execução deste trabalho, o qual é parte do estudo desenvolvido durante o mestrado no PROFMAT/UFERSA.

Referências

[1] Buchmann, J. A. *Introdução à Criptografia, 1a. ed.* Berkeley, São Paulo, 2002.

[2] França, W. B. A. A utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa, 63f, Dissertação de Mestrado, UNB, 2014.

[3] Medeiros, W. S. A arte dos códigos secretos em sala de aula: explorando conceitos de matemática básica em criptografia, 162f, Dissertação de Mestrado, UFERSA, 2020.