

Uma adaptação da Cifra de Hill para estudo de matrizes.

MARIANA MARTINS DURAES BRANDÃO (Autor), EDNEY AUGUSTO JESUS DE OLIVEIRA (Orientador)

No trabalho em questão são apresentados alguns dos principais resultados matemáticos a respeito de Aritmética Modular, dando ênfase às relações de equivalência e classes residuais. É feito também um estudo sobre matrizes e suas propriedades operacionais; a função determinante é construída e apresentada como instrumento para o cálculo de matrizes inversas. Tais temas são abordados com o intuito de fundamentar os processos matemáticos aplicados para funcionamento da Cifra de Hill. Essa cifra é um dos métodos de criptografia apresentados no trabalho, ao qual demos destaque e desenvolvemos uma atividade prática, voltada para turmas do Ensino Médio. Tal atividade consiste em uma adaptação do jogo "WAR", onde a turma é dividida em duas equipes, vencendo a equipe que conseguir conquistar todos os objetivos propostos no início do jogo. Uma das etapas da atividade proposta, consiste em criptografar e descriptografar o nome dos territórios que deverão conquistados por cada equipe, tais processos são baseados em transformações matriciais, que são a chave do funcionamento da Cifra de Hill. O principal objetivo desse trabalho e da atividade, é despertar o interesse do professor de matemática sobre o estudo de criptografia além de estimular e mostrar, de maneira aplicável para os alunos, os conteúdos de matrizes e alguns resultados importantes que são consequência do Teorema da Divisão Euclidiana.

Instituição de Ensino: Universidade Federal de Ouro Preto