Universidade Federal do Paraná - UFPR
Centro Politécnico
Departamento de Matemática

Seminários Contínuos do Programa de Pós-Graduação em Matemática

28 de setembro de 2018 - 15:30 - Anfiteatro A (Bloco PC)

Generalized Hill Cipher

DIEGO ZONTINI - IFPR - Campus Irati

ABSTRACT. In this work we present a generalization of the famous Hill Cipher, which uses invertible linear transformations to encrypt messages. For this we use the generalized inverse concept of matrices, in particular the {2}-inverse with prescribed range and null space, obtaining a robust and secure encryption system. With this generalization, the null space the {2}-inverse can be chosen with a nonzero dimension, allowing that the same message can be encrypted in several totally different ways without affecting its deciphering, obtaining an unbreakable method.