# Cryptanalysis of the Hill Cipher

Nicolette Siermine and Kayla Novak

## Abstract

The Hill cipher is a well-known block cipher that was developed in 1929 by mathematician Lester Hill. It uses invertible matrices and matrix multiplication over finite rings to convert intelligible plaintext into apparently unintelligible ciphertext with the intent of keeping the plaintext secure even if the ciphertext is discovered by an adversary. Previous researchers have been able to attack the Hill cipher with matrices up to size 4 x 4. Our goal is to improve on the attacks done in the past so that we can handle much larger matrices as well as to determine a method for computing the size of the matrix based only on Hill ciphertext. Using the computer programs of Mathematica and Java, we have been implementing an approach using hidden Markov models and testing it on substitution ciphers. We hope to refine this approach in order for it to work with cryptanalyzing the Hill cipher.