Final Project | Encryption

MAT-220-A - Linear Algebra

Brandon Leslie, Shayaan Ahmed, Hershil Patel, Lucas Minnihan

Introduction

As the digital world starts to become more common in everyday life, the protection of sensitive information has become a fundamental priority. **Encryption**, the process of converting data into ineligible code to protect unauthorized access to sensitive information, is a critical tool in protecting digital information. Some commonly protected datatypes include... **IP Addresses, banking information, social security numbers, and more.**

While encryption has heavily relied upon basic number theory and computational algorithms, the evolving complexity of cyber threats, as well as the immense power behind quantum computing & AI, has challenged growth in some areas, prompting the development of new mathematical frameworks. One of these frameworks is **Linear Algebra**, a key branch of mathematics that enables advanced encoding/transformation techniques.

This project investigates how linear algebra can be applied to modern encryption methods. By comparing the mathematical properties of three well known encryption systems (Hill Cipher, RSA, and AES), we aim to understand the inner workings behind the encryption of data and how linear algebra might apart to meet future cyber security demands.

Encryption Methods

Hill Cipher Encryption

- **Hill Cipher**
  - Crated by Lester Hill Cipher circa **1929**
  - Earliest form of computational encryption that utilizes linear algebra
  - **Block Cipher,** encrypts blocks of letters at a time instead of encrypting letter by letter (which is common).

RSA Encryption

AES Encryption

AI & Quantum Computing Usage

Conclusion