(EstablishedunderKarnatakaActNo.16of2013)
B.Tech., 4th Semester, March 2022

LINEAR ALGEBRA PROJECT

by

Name: Vishwas M

SRN: PES2UG20CS390

SEC: F

Team mates: i)V Raghav Loknath
ii) Vishnudeep MR

Report Submitted to the Faculty

Computer Science

Advisor(s): Dr. Girish.

Bangalore, India

April 2022

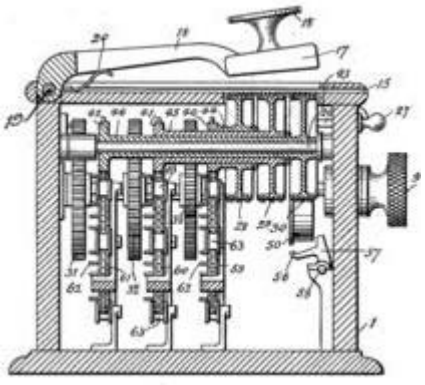
TABLE OF CONTENTS

INTRODUCTION

This paper reports on a simple model for Linear Algebra project, we have found this model to be effective in secured cryptography and reducing the complexity of the development process. Further, this approach requires no complex Mathematical formula , the model is easy to explain and simple to grasp—it has intuitive appeal for people of a technical orientation.

Hill cipher is a multilettered cipher classical encryption technique developed by the mathematician Lester Hill in 1929. It is a poly-graphic substitution cipher based on linear algebra, which has a few advantages in data encryption. But it is vulnerable to known plaintext attack. Further an invertible key matrix is needed for decryption. We have developed our own method for key generation since it has been problematic to choose a random Key matrix..

Hill cipher machine



METHODS

To perform encryption, K must be a square matrix and the inverse of square matrix called decryption matrix using Hill cipher, K must satisfy two important criteria viz., it must be invertible and **gcd(det[K], p)=1** where p is the base value of encoding scheme. In order to generate K for Hill cipher, K is normally obtained randomly and it could not be sometimes invertible. There is no deterministic method yet available in generating K. Thus, this method focuses on a deterministic method in generating K.

Key selection:

We have used a cubic polynomial equation, which on substituting randomized values checks for its invertibility and **gcd(det[Key], p)=1** properties , where p is the base value of encoding scheme.

- $\forall i, if\ MS(i, i), i = 1, \dots, k\ is\ already\ even, leave\ as\ it\ is$
- $. Otherwise, MS(i, i) \leftarrow MS(i, i) + 1\ 5\ 9\ \forall i, if\ MS(i,i)\ is\ already\ even, leave\ as\ it\ is.$
- $Otherwise, MS(i,i) \leftarrow \{ MS(i,i) + 1, i = 1,2, \dots, (k-1)\ MS(n, n) \leftarrow MS(n, n) + 1\ 6\ 8\ \forall i, if\ MS(i, i), i = 1,2, \dots, n-3, n\ is\ already\ even, leave\ as\ it\ is.$
- $Otherwise, MS(i, i) \leftarrow \{ MS(i, i) + 1, when\ i = (n-2), (n-1)$

If the above criteria is satisfied we go on for our encryption and decryption process.

ENCRYPTION AND DECRYPTION

Encryption Algorithm

Step1: Start

Step 2: Input: Plaintext, Key Matrix,

Step 3: Convert the plaintext characters in to matrix form P

Step 3: Perform Encryption using C = KP MOD 26 Where C & P are the matrices of order 1 X N.

Also K is a matrix of the order NXN.

Decryption Algorithm

Step1: Start

Step 2: Input : Ciphertext, Key matrix

Step 3: Calculate inverse key. If the determinant of the Key matrix is zero> Then set offset as follows: If

(Determinant > =0) Then set offset =1 Else Set offset = -1

Step 4: Decryption: P = CK-1 Mod 26

DISCUSSION

Consider the message 'ACT', and the key below (or GYBNQKURP in lette

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'POH'. Now, suppose that our messa

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

ciphertext = 'FIN'

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \pmod{26} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

which gets us back to 'ACT', as expected.

After testing the Hill Cipher algorithm against the plaintext ACT it can be seen that the ciphertext generated through the encryption process can be returned to plaintext correctly without losing a single character. With this, the Hill Cipher algorithm works well with the use of text-based messages.

The basic Hill cipher is vulnerable to a be known as plain text attack because it is completely linear . An opponent who intercepts n^2 plaintext/ciphertext character pairs can set up a linear system which can (usually) be easily solved; if it happens that this system is indeterminate, it is only necessary to add a few more plaintext/ciphertext pairs. Calculating this solution by standard linear algebra algorithms then takes very littletime.

RESULTS

The HILL-cipher method being discussed here is a powerful method and the first general method for successfully applying algebra -specifically linear algebra. The applications of algebra in cryptography is a lot and hill cipher is just an example of it. Unfortunately, the basic Hill cipher is vulnerable to a known-plaintext attack because it is completely linear. While matrix multiplication alone does not result in a secure cipher it is still a useful step when combined with other non-linear operations, because matrix multiplication can provide diffusion.

BIBLIOGRAPHY

Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher(2017)

https://ieeexplore.ieee.org/abstract/document/8074491

A.P. U. Siahaan, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," Int. J. Adv. Appl. Sci., vol.6

.W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice Hall, 2005