Applications of Linear Algebra
Data Encryption

Scott Gregory MATH 308

Abstract

The application of Linear Algebra that is being reviewed is in regards to data encryption. Many corporations, government agencies and educational institutions rely on the ability to keep data from prying eyes. In the effort to keep the data safe one possible solution is to encrypt the data using complicated mathematical algorithms. The problem that is performed below is extremely simple, but when applied on a much larger scale one could see the challenges presented. In my application the key will be a 2x2 invertible matrix, but the United States government uses the DES standard. The key consists of a sixty four bit mathematical algorithm. Only fifty six are actually used in encryption, the rest are used for error checking. The number of possible combinations are in the area of seventy quadrillion. Even if one of fifty six are revealed, there still exists a high probability of security. There was a book written about key codes, "The Code Book" written by Simon Singh, along with a 10,000 pound reward for cracking the 10 levels of encryption. The book describes the rise and fall of empires based on the cracking of codes. My application is simple, but possible through the manipulation of linear algebra.

Application Problem

I found references to this problem within Harvard Math website. In simple terms the alphabet is converted into 28 distinct numbers. There are 26 letters in the alphabet, but with the addition on field it add a level of confusion to a potential hacker.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	

Using the reference word "SPACE" add one space to make the matrix even. This translates into the matrix:

18	0	4
15	2	28

The work is done performed through Maple6:

Linear Algebra Application - Encryption

Scott Gregory - MATH 308

Below is a series of computations to encrypt and decrypt information stored within a matrix.

```
> with(LinearAlgebra):
K:= Matrix([[2,4],[1,7]]);
```

This is the Key for first sample

$$K := \begin{matrix} 2 & 4 \\ 1 & 7 \end{matrix}$$

> **Ki:= MatrixInverse(K);**

The inverse of the key provides a translation tool

$$Ki := \begin{bmatrix} \frac{7}{10} & \frac{-2}{5} \\ \frac{-1}{10} & \frac{1}{5} \end{bmatrix}$$

> **P:= Matrix([[18,0,4],[15,2,28]]);** This is the translated message of SPACE.

$$P := \begin{bmatrix} 18 & 0 & 4 \\ 15 & 2 & 28 \end{bmatrix}$$

> **C:= K.P;** This is the translation from SPACE = JHIOE.

$$C := \begin{bmatrix} 96 & 8 & 120 \\ 123 & 14 & 200 \end{bmatrix}$$

> **TestC:= Ki.C;**

This is the conversion from JHIOE. to SPACE

$$TestC := \begin{bmatrix} 18 & 0 & 4 \\ 15 & 2 & 28 \end{bmatrix}$$

You can see that TestC is the reverse of the original encrypted text
Given the two terms MATH=M, and the encrypted message PHAT=C
Determine the Key Code.

> **M:= Matrix([[12,19],[0,7]]);** Translation: MATH

$$M := \begin{bmatrix} 12 & 19 \\ 0 & 7 \end{bmatrix}$$

> **C:= Matrix([[15,0],[7,19]]);** Translation: PHAT

$$C := \begin{bmatrix} 15 & 0 \\ 7 & 19 \end{bmatrix}$$

> **Key:= MatrixInverse(M).C;** M^-1*C=Key

$$Key := \begin{bmatrix} \frac{-1}{3} & \frac{-361}{84} \\ 1 & \frac{19}{7} \end{bmatrix}$$

this is the key, very simple translation, but by increasing the size of the matrix and the variables high levels of encyption can be achieved.

> **Mtest:= M.Key;**

$$Mtest := \begin{bmatrix} 15 & 0 \\ 7 & 19 \end{bmatrix}$$

This is the test that confims the results.