LINEAR TRANSFORMATION AND ITS APPLICATIONS IN COMPUTER

CHUKWUEDO FAVOUR
EU/SC/MTH/13/007

A PROJECT SUBMITTED TO THE DEPARTMENT OF PHYSICAL SCIENCES COLLEGE OF SCIENCE EVANGEL UNIVERSITY AKAEZE IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE DEGREE IN MATHEMATICS

SEPTEMBER, 2017

LINEAR TRANSFORMATION AND ITS APPLICATIONS IN COMPUTER

CHUKWUEDO FAVOUR
EU/SC/MTH/13/007

A PROJECT SUBMITTED TO THE DEPARTMENT OF PHYSICAL SCIENCES COLLEGE OF SCIENCE EVANGEL UNIVERSITY AKAEZE IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE DEGREE IN MATHEMATICS

SEPTEMBER, 2017

CERTIFICATION

CHUKWUEDO FAVOUR, an Undergraduate in the DEPARTMENT of PHYSICAL SCIENCES (MATHEMATICS OPTION) with registration number EU/SC/MTH/13/007 has satisfactorily completed the requirements for research work for the degree BACHELOR of SCIENCE in MATHEMATICS. The work embodied in this project report is original and has not been submitted in part or full for any other diploma or degree of this or any other university.

MR A. C. ONAH
Project Supervisor

PROF.G. A. AGBO
Head of Department

PROF. OYESANYA, M.O
External Examiner

DEDICATION

To
Almighty God.

ACKNOWLEDGEMENT

How can one ever acknowledge academic debts satisfactorily? Knowledge is a result of a cumulative process spanning over many years during which an individual passes through many people, circumstances and ideas. It is very difficult to categorise them because where the influence of one stops, that of the other begins. But all the same, I wish to express my gratitude to God for making all things well and to a number of people who in one way or the other have been instrumental to the success of this project.

I offer a deserving bow to my supervisor , Mr A.C. Onah for his assistance, invaluable suggestions, painstaking guidance, devotion, constant motivation, patience and loving kindness. He deserves more gratitude from me than I can express here. I am also very grateful to the Members of Staff of the Department of Mathematics, Evangel University Akaeze, Ebonyi State. Prof. U. A. Osisiogu, Dr. J. Ezeora, Mr. R.C Ogbonna, Mr. J. Ofoma and Mr. C. Achudume for their contributions that guided me in the course of this work My special appreciation goes to my parents Mr and Mrs Francis Chukwuedo and my siblings Esther, Gideon, Goodness and Samuel for their financial Support, love, understanding and prayers that created an emotional and conducive surrounding for positive work.

There is no way that I can adequately acknowledge the influence of my course mates Uwaoma David, Nwachi Promise, Wonders Abbah, Okwese Peter and Ogueri Chimezie and my friends for their encouragement.

I do hope that you will tolerate my excesses in the likes of overstatements, understatements, omissions and commissions, some of which hinge on inadequacy of information and personal limitations at a particular time. There is no doubt that I have bitten more than I can chew. In spite of this, I still insist on calling this project "our project", but the lapses remain solely my responsibility.

ABSTRACT

Cryptography, the science of encrypting messages in secret codes, has played an important role in securing information since the emergence of computers. The basic idea of cryptography is that information can be encoded using an encryption scheme and can be decoded by anyone who knows about the scheme. There are lots of encryption schemes ranging from very simple to very complex. Most of them are mathematical in nature. Since matrices together with the linear transformation they represent have unique and very powerful concept such as inverses which can be easily understood, it could be applied as an efficient way for encrypting and storing text. This project work describes some of the techniques of cryptography using matrices together with linear transformation represented. The technique is very simple and can be easily used for encryption of messages confidentially but also not so easy to break if someone does not know the encryption key. The encryption system uses different type of matrices to store the text entered by the sender in the form of their positions and their inverses for decoding the encrypted data into plain-text. Singh et al (2016), considered using an improved matrix cryptography to solve this challenge of security. It requires the key matrix and its inverse in encryption and decryption respectively.

Contents

Certification **i**

Dedication **ii**

Acknowledgement **iii**

Abstract **iv**

1 Introduction **3**

1.1 Background of the Study 3

1.2 Definition Of Terms And Introduction Of Basic Concepts 4

1.2.1 Plain-text 4

1.2.2 Cipher-text 4

1.2.3 Encryption 4

1.2.4 Decryption 4

1.2.5 Cipher 4

1.2.6 **Axioms** 5

1.2.7 Axiom relating Addition and Multiplication 6

1.3 **Field** 6

2 Literature Review **8**

2.1 **Vector Space and Subspace of Vector Space** 9

2.1.1 Vector Space 9

2.1.2 Examples of vector spaces 9

2.1.3 Subspace of Vector Space 13
2.1.4 Examples of Subspaces of vector Spaces 13
2.2 **Linear Combination** 14
2.2.1 Example 14
2.3 **Linear Independent and Linear Dependent Vectors:** 15
2.4 **Spanning Sets and Bases:** 15
2.4.1 Basis 16
2.4.2 Examples of Basis 16

3 Linear transformations **21**
3.1 Properties of linear transformations 22
3.2 **Algebra Of Linear Transformation** 23
3.3 Range Space and Null Space of a Linear Transformation 26
3.3.1 **Example** 27
3.4 **REPRESENTATION OF LINEAR TRANSFORMATION BY MATRICES** 28
3.4.1 Theorem 28
3.5 Linear Transformation Given By Matrices 29

4 Application And Conclusion **30**

Chapter 1

Introduction

1.1 Background of the Study

People all over the world are engaged in communication through internet every day. It is very important to protect our essential data from unauthorized users. The main challenge in data communication is how to keep data secure against unlawful interference often called hacking or eavesdropping. One of the common serious attacks occurs when an unauthorized party can access to read and in some cases, modify an important data. The data transferred from one system to another system over the public network can be protected by means of encryption. Each encryption creates cipher text that can be decrypted into plain-text. Raja and Chakravarthy 2011 used Hilbert matrices to encrypt secret messages and its inverse to decrypt the message. The idea they had behind choosing the Hilbert matrices is that they are always invertible and have integer inverses .

Vector spaces are one of the two main ingredients making up the foundation of this project work, the other being linear transformations. Linear transformations are functions that send, or map, one vector to another vector. Linear refers to the fact that the transformation preserves vector addition and scalar multiplication. This means that if T is a linear transformation sending a vector v to T(v), then for any vectors v and w, and any scalar c, the transformation must satisfy the properties $T(v+w) = T(v)+T(w)$ *and* $T(cv) = cT(v)$.

When doing computations, linear transformations are treated as matrices. The application of linear transformation in computer (*An approach to Cryptography - a data security technique*) as described in this project work stands firm on the basis of the Theorem of The Matrix Representation of a linear transformation.

"Let V be a finite-dimensional vector space over the field F and let $\{v_j\}_{j=1}^n$ be an ordered basis for V. Let W be a vector space over the same field and let $\{v_j\}_{j=1}^n$ be any given vectors in W . Then there exists a unique linear transformation T from V into W such that $Tv_j = w_j, j = 1, 2, 3, ..., n$"

1.2 Definition Of Terms And Introduction Of Basic Concepts

1.2.1 Plain-text

The message or information that is being encrypted.
Example: Any written word

1.2.2 Cipher-text

The message or information that is created after the cipher has been used.

1.2.3 Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

1.2.4 Decryption

Decryption is the process of converting the cipher text (data) to the original plain text(data)(Wu T. M., 2005).

1.2.5 Cipher

A procedure that will render a message unintelligible to the recipient. Used to also recreate the original message.

Example:

plaintext: 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
ciphertext: X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

In this example, the message:

WHAT KIND OF CAKE SHOULD WE HAVE? ALICE.

will be rendered as follows:

TEXQ HFKA LC ZXHB PELRIA TB EXSB? XIFZB.

1.2.6 Axioms

Laws governing the way numbers combine together are called axioms. Any particular axiom might be true in some number systems but not in others.

Axioms for Addition

Let S be a number system;

A1. $\alpha + \beta = \alpha + \beta \ \forall \ \alpha \ , \beta \in S$.

A2. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \ \forall \ \alpha, \beta, \gamma \in S$.

A3. There is a number $0 \in S$ such that $\alpha + 0 = 0 + \alpha = \alpha \ \forall \ \alpha \in S$.

A4. For each number $\alpha \in S \ \exists$ a number $-\alpha \in S$ such that $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$.

These axioms may or may not be satisfied by a given number system S. For example, in N, A1 and A2 hold but A3 and A4 do not hold. A1 - A4 all hold in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Axioms for Multiplication

Let S be a number system;

M1. $\alpha.\beta = \beta.\alpha \ \forall \ \alpha, \beta \in S.$

M2. $(\alpha.\beta).\gamma = \alpha.(\beta.\gamma) \ \forall \ \alpha, \beta, \gamma \in S.$

M3. There is a number $1 \in S$ *suchthat* $\alpha.1 = 1.\alpha = \alpha \forall \alpha \in S.$

M4. For each number $\alpha \in S$ with $\alpha \neq 0, \exists$ a number $\alpha^{-1} \in S$ such that $\alpha.\alpha^{-1} = \alpha^{-1}.\alpha = 1.$

In $\mathbb{N}$ and $\mathbb{Z}$, M1-M3 hold but M4 does not hold. M1-M4 all hold in $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

1.2.7 Axiom relating Addition and Multiplication

D. $(\alpha + \beta).\gamma = \alpha.\gamma + \beta.\gamma \ \forall \ \alpha, \beta, \gamma \in S$

1.3 Field

Definition. A field is a non-empty set, on which two binary operations $+$ *and* $\bullet$ called addition and multiplication, respectively, are defined.
Concurrently, a set S on which addition and multiplication are defined is called a field if it satisfies each of the axioms A1, A2, A3, A4, M1, M2, M3, M4, D, and if, in addition, $1 \neq 0$.

Roughly speaking, S is a field if addition, subtraction, multiplication and division(except by zero) are all possible in S. Elements of a field are often called **Scalars**.

Examples of fields include

(a) The set of all real numbers $\mathbb{R}$ with the usual addition and multiplication.

(b) The set of all rational numbers $\mathbb{Q}$ with the usual addition and multiplication on $\mathbb{R}$.

(c) The set of all complex numbers $\mathbb{C}$ with the usual addition and multiplication on complex numbers.

Chapter 2

Literature Review

During the last decades, information security has become a major issue (Obaida Mohammad Awad Al-Hazaimeh 2013). With the rapid development of network and multimedia technologies, the digital information has been applied to many areas in real-world applications. Communication has become a very important aspect in today's life. So, security plays an important role in transferring the data. One such way to secure information is cryptography. In this parlance, the theorem of the matrix representation of a linear transformation becomes very useful. In cryptography we hide the information from unauthorized users by employing various techniques, encryption is one such technique where we transform the data into a form understandable only by the authorized users. We need to hide the data for privacy purpose and for ensuring data received at the authenticated user end is not modified .We have several encryption and decryption algorithms for encrypting the data at sender end and decrypting the same at receiver side ensuring secure data transfer.

2.1 Vector Space and Subspace of Vector Space

2.1.1 Vector Space

A vector space over a field K is a set V which has two basic operations, addition and scalar multiplication, satisfying certain requirements. Thus for every pair $u, v \in V,\ u+v \in V$ is defined, and for every $\alpha \in K,\ \alpha v \in V$ is defined. For V to be called a vector space, the following axioms must be satisfied for all $\alpha, \beta \in K$ and all $u, v \in V$. In this project, unless otherwise stated, scalars are chosen from the set of real numbers.

Vector addition satisfies axioms A1, A2, A3 and A4 above.

$\alpha(u+v) = \alpha u + \alpha v$;

$(\alpha+\beta)v = \alpha v + \beta v$;

$(\alpha\beta)v = \alpha(\beta v)$;

$1v = v$.

If V is a vector space over the field of real numbers, $\mathbb{R}$, then V is called a real vector space. V is called a complex vector space if V is a vector space (over $\mathbb{C}$) the field of complex numbers.

2.1.2 Examples of vector spaces

Examples of Vector Spaces

1. Let **f** be any field and $f^n = f \times f \times ... \times f$ (**n** factors of **f**)

   $x \in f \Rightarrow x = (x_1, x_2, ..., x_n); x_i \in f, \forall i = 1, 2, ..., n)$i.e.

   $$f^n = \{(x_1, x_2, ..., x_n) : x_i \in f, \forall i = 1, 2, ..., n)\}$$

   define addition and scalar multiplication on $\mathbf{f}^n$ by

   $$x + y = (x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)$$

   $$= (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$$

   $$\alpha x = \alpha(x_1, x_2, ..., x_n) = (\alpha x_1, \alpha x_2, ..., \alpha x_n)$$

for all $x = (x_1, x_2, ..., x_n)\,; y = (y_1, y_2, ..., y_n) \in f^n \; and \; \alpha \in f$

With this addition and scalar multiplication**,** $\mathbf{f}^n$ is a vector space.

Verification:

Let $x, y, z \in f^n$ and $\alpha, \beta \in f$; be arbitrary such that

$$x = (x_1, x_2, ..., x_n); y = (y_1, y_2, ..., y_n); z = (z_1, z_2, ..., z_n)$$

Closure under addition

(i) $x + y = (x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)$

$= x + y = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n) \in f^n$, since each $x_i, y_i \in f$ and so is $x_i + y_i$

(ii) Closure under scalar multiplication

$\alpha x = \alpha(x_1, x_2, ..., x_n) = (\alpha x_1, \alpha x_2, ..., \alpha x_n) \in f^n$, since $\alpha x_i \in f$ for each **i**

(iii) Commutativity under addition

$$x + y = (x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)$$

$$= (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$$

$$= (y_1 + x_1, y_2 + x_1, ..., y_n + x_n)$$

$$= (y_1, y_2, ..., y_n) + (x_1, x_2, ..., x_n)$$

$$= \mathrm{y} + \mathrm{x}$$

(iv) Associativity under addition.

$$(x + y) + z = [(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)] + (z_1, z_2, ..., z_n)$$

$$= [(x_1 + y_1, x_2 + y_2, ..., x_n + y_n)] + (z_1, z_2, ..., z_n)$$

$$= [x_1 + y_1 + z_1, x_2 + y_2 + z_2 +, ..., + x_n + y_n + z_n]$$

$$= [x_1 + (y_1 + z_1), x_2 + (y_2 + z_2) +, ..., + x_n + (y_n + z_n)]$$

$$= (x_1, x_2, ..., x_n) + [y_1 + z_1, y_2 + z_2, ..., y_n + z_n]$$

$$= x + (y + z)$$

(v) Existence of additive identity.

There exist $0 = (0, 0, ..., 0) \in f^n$ such that

$$0 + x = (0, 0, ..., 0) + (x_1, x_2, ..., x_n)$$

$$= (0 + x_1, 0 + x_2, ..., 0 + x_n)$$
$$= (x, x, ..., x) = x$$

(vi) Existence of additive inverse

Let $x = (x_1, x_2, ..., x_n) \in f^n$ be arbitrary, then, by property of field, there exist $-x = (-x_1, -x_2, ..., -x_n) \in f^n$, such that

$$x + (-x) = (x_1, x_2, ..., x_n) + (-x_1, -x_2, ..., -x_n)$$
$$= (x_1 - x_2, x_2 - x_2, ..., x_n - x_n)$$
$$= (0, 0, ..., 0) = 0$$
$$(vii) : \alpha(x + y) = \alpha(x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$$
$$= [\alpha(x_1 + y_1), \alpha(x_2 + y_2), ..., \alpha(x_n + y_n)]$$
$$= (\alpha x_1 + \alpha y_1, \alpha x_2 + \alpha y_2, ..., \alpha x_n + \alpha y_n)$$
$$= (\alpha x_1, \alpha x_2, ..., \alpha x_n) + (\alpha y_1, \alpha y_2, ..., \alpha y_n)$$
$$= \alpha(x_1, x_2, ..., x_n) + \alpha(y_1, y_2, ..., y_n)$$
$$= \alpha x + \alpha y$$
$$(viii) : (\alpha + \beta)x = (\alpha + \beta)(x_1, x_2, ..., x_n)$$
$$= ((\alpha + \beta)x_1, (\alpha + \beta)x_2, ..., (\alpha + \beta)x_n)$$
$$= (\alpha x_1 + \beta x_1, \alpha x_2 + \beta x_2, ..., \alpha x_n + \beta x_n)$$
$$= (\alpha x_1, \alpha x_2, ..., \alpha x_n) + (\beta x_1, \beta x_2, ..., \beta x_n)$$
$$= \alpha(x_1, x_2, ..., x_n) + \beta(x_1, x_2, ..., x_n) = \alpha x + \beta x$$
$$(ix) : (\alpha x)\beta = [\alpha(x_1, x_2, ..., x_n)\beta]$$
$$= (\alpha x_1, \alpha x_2, ..., \alpha x_n)\beta$$
$$= (\alpha\beta x_1, \alpha\beta x_2, ..., \alpha\beta x_n)$$
$$= \alpha(\beta x_1, \beta x_2, ..., \beta x_n)$$
$$= \alpha[\beta(x_1, x_2, ..., x_n)] = \alpha(\beta x)$$

$$(x) : \exists 1 \in f \ni 1 \bullet x = 1 \bullet (x_1, x_2, ..., x_n)$$
$$= (1 \bullet x_1, 1 \bullet x_2, ..., 1 \bullet x_n)$$
$$= (x_1, x_2, ..., x_n) = x$$

$\therefore$ f^n is a vector space over $\mathbf{f}$

This example shows that the cartesian products $\mathbb{R}^{\times}$, $\mathbb{Q}^{\times}$ *and* $\mathbb{C}^{\times}$ are vector spaces over the fields $\mathbb{R}, \mathbb{Q}$ and $\mathbb{C}$ respectively.

2.1.3 Subspace of Vector Space

Many interesting examples of vector spaces are subsets of a given vector space V that are vector spaces in their own right.

Let V be a vector space over the field K. Certain subsets of V have the nice property of being closed under addition and scalar multiplication; that is, adding or taking scalar multiples of vectors in the subset gives vectors which are again in the subset. We call such a subset a subspace:

Definition. A subspace of V is a non-empty subset $W \subseteq V$ such that

i W is closed under addition: $u, v \in W \Longrightarrow u + v \in W$.

ii W is closed under scalar multiplication: $v \in W, \alpha \in K \rightarrow \alpha v \in W$.

These two conditions can be replaced with a single condition

$$u, v \in W, \alpha, \beta \in K \rightarrow \alpha u + \beta v \in W.$$

A subspace W is itself a vector space over K under the operations of vector addition and scalar multiplication in V . Notice that all vector space axioms of W hold automatically. (They are inherited from V .)

2.1.4 Examples of Subspaces of vector Spaces

1. Let **S** be any real vector space. Then, $\{0\}$ is a subspace of **S**, usually called the **trivial subspace** of any vector space.

   Verification: Given, $V = \{0\}$,then, $x, y \in V; \Rightarrow x = y = 0$ and so

   $$\forall \alpha, \beta \in \Re; \alpha x + \beta y = \alpha(0) + \beta(0) = 0 + 0 = 0 \in V$$

Note that any subspace of V that contains W_1 *and* W_2 has to contain all vectors of the form $u + v$ for $u \in W_1,\ v \in W_2$. This motivates the following definition.

Definition. Let W_1, W_2 be subspaces of the vector space V . Then $W_1 + W_2$ is defined to be the set of vectors $v \in V$ such that $v = w_1 + w_2$ *for some* $w_1 \in W_1, w_2 \in W_2$.

Or Preferably, $W_1 + W_2 = w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2$.

2.2 Linear Combination

Given that $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$are scalars in a scalar field $F$and $v_1, v_2, v_3, \ldots, v_n$are vectors in a vector space, Vover the scalar field. Then, the linear combination of $v_1, v_2, v_3, \ldots, v_n$ (with those scalars as coefficients) is an expression of the form

$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \ldots + \lambda_n v_n$ or $\sum_{k=1}^{n} \lambda_k v_k$ in compact form. In line with this, a given vector $v \in V$ is said to be a linear combination of a set of vectors $v_1, v_2, v_3, \ldots, v_n$if there exists scalars $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ such that $v = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \ldots + \lambda_n v_n$.

2.2.1 Example

1. Let the field K be the set of real numbers. Let the vector space V be the Euclidean space, $\Re^3$. Consider the vectors, $e_1 = (1, 0, 0),\ e_2 = (0, 1, 0) and\ e_3 = (0, 0, 1)$. Then, any vector in $\Re^3$ is a linear combination of e_1, e_2 *and* e_3

Verification: Let $v = (\alpha_1, \alpha_2, \alpha_3)$be arbitrary. We seek scalars λ_1, λ_2 *and* $\lambda_3$such that $(\alpha_1, \alpha_2, \alpha_3) = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$. This means that,

$$\begin{aligned}(\alpha_1, \alpha_2, \alpha_3) &= \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 \\ &= \lambda_1(1, 0, 0) + \lambda_2(0, 1, 0) + \lambda_3(0, 0, 1) \\ &= (\lambda_1, 0, 0) + (0, \lambda_2, 0) + (0, 0, \lambda_3) \\ &= (\lambda_1, \lambda_2, \lambda_3)\end{aligned}$$

Which implies that $\lambda_1 = \alpha_1,\ \lambda_2 = \alpha_2$ *and* $\lambda_3 = \alpha_3$.

2.3 Linear Independent and Linear Dependent Vectors:

Let **V** be a real vector space. The vectors $v_1, v_2, ..., v_n$in **V** are said to be linearly independent over R if for $t_1, t_2, ..., t_n$ in **R**, we have

$\sum_{k=1}^{n} t_k v_k = 0$ implies that$t_1 = t_2 = ... = t_n = 0$.

Vectors which are not linearly independent are said to be linearly dependent.

In a linearly dependent set of vectors one can express at least one of the vectors as a **linear combination** of the others. While, this is not possible in a linearly independent set of vectors. If we want to check whether a set of vectors $v_1, v_2, ..., v_n$ is linearly independent or not, we form a linear combination $\sum_{k=1}^{n} t_k v_k$of the vectors and assume this to be zero and then solve for $t_1, t_2, ..., t_k$. If all the **t's** are zero, then our set of vectors is linearly independent, otherwise, it is linearly dependent.

Example

1. In the vector space $\mathbb{R}^{\kappa}$, the following set of vectors
   $S = \{e_i = (0, 0, ..., 0, 1, 0, 0, ..., 0); i = 1, 2, ..., n\}$, (with **1** in the ith entry) is linearly independent .

   Verification: Without loss of generality, in $\mathbb{R}^{\nVdash}$,

$$S = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}.$$
$$\text{Let } v_1 = (1, 0, 0), v_2 = (0, 1, 0), v_3 = (0, 0, 1); t_1, t_2, t_3 \in R$$

$$\text{Then, } \textstyle\sum_{k=1}^{3} t_k v_k = 0, \text{ implies that}$$

$$t_1(1, 0, 0) + t_2(0, 1, 0) + t_3(0, 0, 1) = (0, 0, 0)$$
$$\Rightarrow (t_1, t_2, t_3) = (0, 0, 0)$$
$$\Rightarrow t_1 = 0; t_2 = 0; t_3 = 0$$

2.4 Spanning Sets and Bases:

Let **V** be a real vector space and $S = \{v_1, v_2, ..., v_n\}$ a subset of **V**. The span of **S** denoted by **span[s]** is the set of all finite **linear combinations** of the vectors, $v_1, v_2, ..., v_n$, i.e. $Span[s] = \{v \in V : v = \sum_{k=1}^{n} t_k v_k; t_k \in R, k = 1, 2, ..., n\}$

2.4.1 Basis

A **basis** for a vector space **V** over **R** is a linearly independent subset of **V** which spans **V**.

2.4.2 Examples of Basis

- Let $V = R^3$ and $S = \{(1, 2, 0), (-1, 1, 0)\}$. What is **span[S]** ?
- Find the span of the vector $(-1, 1)$.
- Find the span of $S = \{(1, 1, 0), (-1, 0, 0)\}$

Solution

The solution to the above can only be completed by the preceding theorem.

Theorem

Let **V** be a vector space over R, and let $S = \{v_1, v_2, ..., v_n\}$ be a subset of **V**. Then

- **Span[S]** is a subspace of V.
- If **S** is linearly independent, then every vector in **span[S]** can be written in only one way as a linear combination of the vectors in **S**.
- If **S** is linearly independent and **y** is not in **span[S]** then the set obtained by adding **y** to **S** is linearly independent.

A set of vectors $S = \{v_1, v_2, ..., v_n\}$ in **V** is said to generate or span **V** if every vector in **V** can be expressed as a linear combination of $v_1, v_2, ..., v_n$, i.e. if **v** is an arbitrary element of **V**, then there exist $t_1, t_2, ..., t_k \in R$ such that $v = \sum_{k=1}^{n} t_k v_k$, i.e , $V = span[S]$. In other words, a subset of a vector space is said to span (or generate) the vector space if for every vector in the vector space, one can find suitable scalars such that the vector can be expressed as alinear combination of the vectors in the subset.

A **basis** for a vector space **V** over **R** is a linearly independent subset of **V** which spans **V**.

Examples

- In the vector space $\mathbb{R}^{\kappa}$, the set of vectors $S = \{e_i = (0, 0, ..., 0, 1, 0, 0, ..., 0); i = 1, 2, ..., n\}$, (with **1** in the ith entry) is a basis for $\mathbb{R}^{\kappa}$ (why?). The set of vectors $S = \{e_1, e_2, ..., e_n\}$ is called the usual or standard basis for $\mathbb{R}^{\kappa}$.

- The set of vectors $S = \{(1,1,1),(0,1,2),(0,0,1)\}$is a basis for $\mathbb{R}^{\not\vDash}$ (why?).
- The set of vectors $S = \{(1,1,1),(0,1,2),(0,0,1)\}$ is a basis for $\mathbb{R}^{\not\vDash}$ (see example (i)).
- In $\mathbf{R}$ any set consisting of just one non-zero number is a basis.
- The set $\{(1,0,0),(0,1,0),(1,1,0)\}$is not a spanning set of $\mathbb{R}^{\not\vDash}$ instead its span is the space of all vectors in $\mathbb{R}^{\not\vDash}$ whose last component is zero.
- In $\mathbb{R}^{\not\vDash}$, the vectors $v_1 = (1,1)$ *and* $v_2 = (-1,2)$is a basis for $\mathbb{R}^{\not\vDash}$.

To illustrate with example (iv), we have to prove that these two vectors form a basis for $\Re^2$. To this end, it suffices to prove that these vectors are linearly independent and that they generate (or span) $\Re^2$.

Part I: Recall that two vectors v_1 *and* v_2 are linearly independent if $\lambda_1 v_1 + \lambda_2 v_2 = 0$ with (λ_1 *and* λ_2 being scalars) implies that $\lambda_1 = 0$ *and* $\lambda_2 = 0$. Hence, to prove that $(1,1)$ *and* $(-1,2)$ are linearly independent, we assume that there exists scalars λ_1 *and* λ_2 such that $\lambda_1(1,1) + \lambda_2(-1,2) = (0,0)$and strive to show that $\lambda_1 = \lambda_2 = 0$. But,
$\lambda_1(1,1) + \lambda_2(-1,2) = (0,0)$
$\Rightarrow (\lambda_1, \lambda_1) + (-\lambda_2, 2\lambda_2) = (0,0)$
$\Rightarrow (\lambda_1 - \lambda_2, \lambda_1 + 2\lambda_2) = (0,0)$
$\Rightarrow \lambda_1 - \lambda_2 = 0$ *and* $\lambda_1 + 2\lambda_2 = 0$

On solving, we have that$\lambda_1 = 0$ *and* $\lambda_2 = 0$. Therefore, $(1,1)$ *and* $(-1,2)$ are linearly independent.

Part II: Recall that two vectors v_1 *and* v_2 are said to generate or span a vector space, V**,** over a scalar field F if for every vector, $\vec{v} \in V$, it is possible to find λ_1 *and* $\lambda_2$in Fsuch that $\vec{v} = \lambda_1 v_1 + \lambda_2 v_2$. Hence, to prove that $(1,1)$ *and* $(-1,2)$ span $\Re^2$, we assume that $\vec{v} = (x,y)$ is an arbitrary vector in $\Re^2$ and seek λ_1 *and* $\lambda_2$in Fsuch that $\lambda_1 v_1 + \lambda_2 v_2 = (x,y)$ But,

$$\begin{aligned}
&\lambda_1 v_1 + \lambda_2 v_2 = (x,y)\\
&\Rightarrow \lambda_1(1,1) + \lambda_2(-1,2) = (x,y)\\
&\Rightarrow (\lambda_1, \lambda_1) + (-\lambda_2, 2\lambda_2) = (x,y)\\
&\Rightarrow (\lambda_1 - \lambda_2, \lambda_1 + 2\lambda_2) = (x,y)\\
&\Rightarrow \lambda_1 - \lambda_2 = x \text{ and } \lambda_1 + 2\lambda_2 = y
\end{aligned}$$

On solving for λ_1 *and* λ_2 by subtracting the last two equations, we have that $3\lambda_2 = y - x$which in turn implies that $\lambda_2 = \frac{1}{3}(y-x)$and on substitution followed by simplification, we have that $\lambda_1 = \frac{1}{3}(y+2x)$. Therefore, $(1,1)$ *and* $(-1,2)$ span $\Re^2$ because for any vector $\vec{v} = (x,y) \in \Re^2$, we can find $\lambda_1 = \frac{1}{3}(y+2x)$ and $\lambda_2 = \frac{1}{3}(y-x)$both in F such that $(x,y) = \frac{1}{3}(y+2x)(1,1) + \frac{1}{3}(y-x)(-1,2)$.

Theorem

Let **V** be a vector space that has a basis consisting of **n** vectors. Then,

i any set with more than **n** vectors is linearly independent

ii any spanning set has at least **n** vectors

iii any linearly independent subset of **V** has at most **n** vectors

iv every basis of $\mathbf{V}$ contains exactly $\mathbf{n}$ vectors

Proof

Let **V** be a real vector space. We say that the dimension of **V** is **n** , $\dim(V) = n$, if **V** has a basis of **n** vectors. If **V** is the vector space that consists of the zero vector only, we define the dimension of **V** to be **0**. If $\dim(V) = n$, we call **V** an n-dimensional vector space.

If for any **n**, **V** has a set of **n** linearly independent vectors, we say that the dimension of **V** is infinite. The set, of all polynomials with coefficients from **R** is infinite dimensional. The set of all real-valued functions defined on $[a, b]$ is also infinite dimensional.

Chapter 3

Linear transformations

Definition. Let V and W be real vector spaces. A Linear transformation from V into W is a function $T : V \longrightarrow W$ which satisfies the following properties.

- $T(x + y) = Tx + Ty; \forall x, y \in V$; **Property 1**

  (We say that T preserves additivity.)

- $T(ax) = aTx; \forall x \in V; \forall a \in R.$ **Property 2**

  (We say that T preserves scalar multiplication.)

If both properties itemised above are satisfied, then, $\forall x, y \in V; \forall a, b \in R$, we have:

$$T(ax + by) = T(ax) + T(by) = aTx + bTy; \forall x, y \in V; a, b \in R$$

Conversely, if

$$T(ax + by) = aTx + bTy; \forall x, y \in V; a, b \in R,$$

then by taking $a = b = 1$ in the equation above we obtain (**Property 1**) and taking $b = 0$ we obtain (**Property 2**).
Thus Property 1 and Property 2 can be replaced by :

$$T(ax+by) = T(ax) + T(by) = aTx + bTy; \forall x, y \in V; a, b \in R$$

It is important to observe that if $a = 0$ in (Property 2), then we obtain $T(0) = 0$. Thus, if $T : V \longrightarrow W$ is a Linear Transformation, then T must take the zero element of V to the zero element of W

The following examples copiously explains the concept.

Example

Let **V** be a given real vector space. Then the **identity operator,** $T : V \to V$ defined for any given $x \in V$ by $Tx = x$ is a linear transformation, since

$T(ax+by) = ax+by \quad (\ from\ definition\ of\ T)$
$= aTx + bTy; \forall x, y \in V; a, b \in R.$

Example

The **zero transformation**, $T : V \to W$ defined for all $x \in V$ by $Tx = 0$ is a linear transformation, since
$T(x+y) = 0 \quad (\ from\ definition\ of\ T)\ = 0+0 = Tx+Ty$, and $T(ax) = 0 = a0 = aTx$.

3.1 Properties of linear transformations

Theorem. Let V *and* W be two vector spaces. Suppose $T : V \longrightarrow W$ is a linear transformation. Then

1. $T(0) = 0$.
2. $T(-v) = -T(v)\ \forall\ v \in V$
3. $T(u-v) = T(u) - T(v)\ \forall\ u, v \in V$
4. If $v = c_1v_1 + c_2v_2 + ... + c_nv_n$ then,

$$T(v) = T(c_1v_1 + c_2v_2 + ... + c_nv_n) = c_1T(v_1) + c_2T(v_2) + ... + c_nT(v_n).$$

3.2 Algebra Of Linear Transformation

Basically this explains some ways of combining linear transformation to get another linear transformation.

Theorem

Let **V** and **W** be real vector spaces and let $\mathbf{T}_1$ and $\mathbf{T}_2$ be linear transformation from **V** into **W**. Then the function $(T_1 + T_2)$ defined for all $x \in V$ by $(T_1 + T_2)(x) = T_1x + T_2x$ is a linear transformation.

If **c** is any element of **R**, then the function $(cT_1) : V \to W$ defined for each $x \in V$ by $(cT_1)(x) = cT_1x$ is a linear transformation from **V** into **W**. Furthermore, the set of all linear transformations defined from **V** into **W** with the addition and scalar multiplication defined above is a vector space.

Proof

Let $x, y \in V; a, b \in R$ be arbitrary. Then,

$$\begin{aligned}(T_1 + T_2)(ax + by) &= T_1(ax + by) + T_2(ax + by)\\ &= aT_1x + bT_1y + aT_2x + bT_2y\\ &= a(T_1 + T_2)x + b(T_1 + T_2)y\end{aligned}$$

Furthermore,

$$(cT)(ax + by) = cT(ax) + cT(by) = a(cT)(x) + b(cT)(y)$$

Let $L(V, W)$ denote the set of all linear transformations from **V** into **W**. we prove that $L(V, W)$ is a vector space. Observe that closure under addition and scalar multiplication has been shown above. The additive identity is the zero transformation which transforms every vector in **V** into the zero-vector in **W**. the rest of the properties corresponding properties of the operations in the space **W**.

Theorem

Let **U, V** and **W** be real vector spaces, and let $T_1 : U \to V; T_2 : V \to W$ be linear transformations. Then, the function $T_2oT_1 = T_2T_1 : U \to W$ and

$T_1oT_2 = T_1T_2 : V \to V$ are linear transformations(if $U \cap V \neq \emptyset$).

Proof: Let $x, y \in V$ and $a, b \in R$ be arbitrary. Then,

$$\begin{aligned}T_2oT_1(ax + by) &= T_2[T_1(ax + by)]\\ &= T_2[aT_1x + bT_1y]\\ &= aT_2(T_1x) + bT_2(T_1y)\\ &= a(T_2T_1)(x) + b(T_2T_1)(y)\end{aligned}$$

The proof that T_1oT_2 is a linear transformation follows similarly.

Invertible Linear Transformation

Theorem

Let V, W be real vector spaces, and $T : V \to W$ a linear transformation. **T** is said to be **invertible** if there exist a function denoted by $\mathbf{T}^{-1}$ defined from **W** into **V** such that ToT^{-1} is the identity transformation on **V** which sent every element of **V** to itself and ToT^{-1} is the identity element of **W** which sends every element of **W** to itself, $\mathbf{T}^{-1}$ is called the inverse of **T**.

Theorem:

If $T : V \to W$ is invertible, then $T^{-1} : W \to V$ is a linear transformation.

Proof Let $y_1, y_2 \in W$ and $a, b \in R$ be, arbitrary. Then we show that$T^{-1}(ay_1 + by_2) = aT^{-1}y_1 + bT^{-1}y_2$. Since,$y_1, y_2 \in W$, and **T** is invertible, then there exists $x_1, x_2 \in V$ such that $Tx_1 = y_1$, and $Tx_2 = y_2$. Hence, $x_1 = T^{-1}y_1$ and $x_2 = T^{-1}y_2$. Then,

$$\begin{aligned} T^{-1}(ay_1 + by_2) &= T^{-1}(aTx_1 + bTx_2) \\ &= T^{-1}[T(ax_1) + T(bx_2)] \\ &= T^{-1}[T(ax_1 + bx_2)] \\ &= ax_1 + bx_2 \\ &= aT^{-1}y_1 + bT^{-1}y_2 \end{aligned}$$

Let $T : V \to W$ be a linear transformation. Then **T** is invertible (one-to-one) if and only if $N(T) = \{0\}$

Proof: Suppose **T** is **1-1**, we prove that $N(T) = \{0\}$. Since **T** is **1-1**, $Tx = Ty$ implies that$x = y$. Let $v \in N(T)$ be arbitrary, then, $Tv = 0 = T0$, so that $Tv = T0 = 0$. Hence, $v = 0$, and consequently $N(T) = \{0\}$.

Conversely, suppose that $N(T) = \{0\}$, we prove **T** is **1-1**.Let $x, y \in V$ be arbitrary and suppose $Tx = Ty$, then $Tx - Ty = 0$. Hence, $T(x - y) = 0$, so that $(x - y) \in N(T) = \{0\}$ from which it follows that $x = y$, completing the proof.

3.3 Range Space and Null Space of a Linear Transformation

Definition

Let **V** and **W** be real vector spaces, and let $T : V \to W$ be a linear transformation. The **range** of **T** which we shall denote by $R(T)$ is the set:

$$R(T) = \{y \in W : Tx = y, for - some, x \in V\} = \{Tx : x \in V\}$$

The **Null Space** (or the **Kernel**) of **T** which we shall denote by $N(T)$

$[or, Ker(T)]$ is the set

$$N(T) = Ker(T) = \{v \in V : Tv = 0\}$$

3.3.1 Example

Let $V = R^3$ and define $T : V \to V$ by

$T(x,y,z) = (x,y,0); \forall (x,y,z) \in V$. Then T is a linear transformation and

$$R(T) = \left\{T(x,y,z) : (x,y,z) \in R^3\right\}$$

$$R(T) = \{T(x,y,z) : (x,y,z) \in R^3\}$$
$$= \{(x,y,0) : x,y \in R\}$$

$$N(T) = \{(x,y,z) \in V : T(x,y,z) = (x,y,0) = (0,0,0)\}$$
$$= \{(0,0,z) : z \in R\} = z - axis$$

Example

let $V = R^2$ and let $A = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}$ Define $T : V \to V$ by $Tx = Ax; \forall x = \begin{bmatrix} x \\ y \end{bmatrix} \in V$.

Then **T** is a linear transformation (from above example)

$$N(T) = \left\{ x \in V : Ax = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}.$$

Observe that $Ax = 0$ implies that $\begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ \text{y} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$

Solving this system of equations now yields: $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ (multiply LHS and apply equality of matrices).

Hence,$N(T) = \{0\}$, (the set containing only the zero vector in v). In this case,

$$R(T) = V.$$

Example

Let $V = R^2$ and let $A = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$, Define $T : V \to V$ by $Tx = Ax; \forall x = \begin{bmatrix} x \\ y \end{bmatrix} \in V$.

Then **T** is a linear transformation

$$N(T) = Span[\begin{bmatrix} -2 \\ 1 \end{bmatrix}]$$

Theorem

Let **V** and **W** be real vector spaces and $T : V \to W$ a linear transformation. Then,

1. **R(T)** is a subspace of **W**.
2. **N(T)** is a subspace of **V.**

Proof

Let $y_{1,}y_2 \in R(T); a, b \in R$ be arbitrary. Then, there exist $x_{1,}x_2 \in V$ such that $Tx_1 = y_1; Tx_2 = y_2$. Since, $ax_1 + bx_2 \in V$ (since V is a vector space) and

$T(ax_1 + bx_2) = aTx_1 + bTx_2 = ay_1 + by_2$. Therefore, $ay_1 + by_2 \in R(T)$.

To prove that **N(T)** is a subspace of **V**, let $v_{1,}v_2 \in N(T)$ be arbitrary. Then, $Tv_1 = Tv_2 = 0$. For any $a, b \in R$, we have $T(av_1 + bv_2) = aTv_1 + Tv_2 = 0$. So that

$(av_1 + bv_2) \in N(T)$, completing the proof.

3.4 REPRESENTATION OF LINEAR TRANSFORMATION BY MATRICES

Let V be an n-dimensional vector space over a field F and let W be an m-dimensional vector space over F. Tentatively, it can be shown that every linear transformation $T : V \longrightarrow W$ could be represented by an $m \times n$ matrix, A. Therefore a detailed study of how such matrix representation of T could be obtained

3.4.1 Theorem

Let V be a finite-dimensional vector space over the field F and let $\{v_j\}_{j=1}^n$ be an ordered basis for V. Let W be a vector space over the same field and let $\{v_j\}_{j=1}^n$ be any given vectors in W . Then there exists a unique linear transformation T from V into W such that $Tv_j = w_j, j = 1, 2, 3, ..., n$

3.5 Linear Transformation Given By Matrices

Suppose A is a matrix of size m x n. Given a vector

$$V = \begin{bmatrix} v_1 \\ v_2 \\ ... \\ v_n \end{bmatrix} \in \mathbb{R}^n \; define \; T(v) = Av = A = \begin{bmatrix} v_1 \\ v_2 \\ ... \\ v_n \end{bmatrix}$$

Then T is a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Proof. From properties of matrix multiplication, for $u, v \in \mathbb{R}^n$ and scalar c we have :

$$T(u+v) = A(u+v) = A(u) + A(v) = T(u) + T(v)$$

and

$$T(cu) = A(cu) = cAu = cT(u).$$

Completing the proof.

Chapter 4

Application And Conclusion

Cryptography, to most people, is concerned with keeping communications private. Indeed, **the protection of sensitive communications** has been the emphasis of cryptography throughout much of its history. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

Application 1

For the security, we first code the alphabet as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1. Next, obtain a Cipher matrix -

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

   For this example we will use the following Plain-text -

PENGUINS ARE ONE TO ONE

2. Now we will replace each letter with its numerical representation, using **1-26** for **A-Z** and **27** for a space between the words. Leaving us with :

16, 5, 14, 7, 21, 9, 14, 19, 27, 1, 18, 5, 27, 15, 14, 5, 27, 20, 15, 27, 15, 14, 5

3. Now separate the Plain-text into **3x1** vectors until the whole Plain-text is used.

[16] [7] [14] [1] [27] [5] [15] [14]
[5] [21] [19] [18] [15] [27] [27] [5]
[14] [9] [27] [5] [14] [20] [15] [27]

4. Augment these vectors into a plaintext matrix -

$$\begin{bmatrix} 16 & 7 & 14 & 1 & 27 & 5 & 15 & 14 \\ 5 & 21 & 19 & 18 & 15 & 27 & 27 & 5 \\ 14 & 9 & 27 & 5 & 14 & 20 & 15 & 27 \end{bmatrix}$$

5. Multiply the **Plain-text matrix** with the **Cipher matrix** to form the encrypted matrix -

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} * \begin{bmatrix} 16 & 7 & 14 & 1 & 27 & 5 & 15 & 14 \\ 5 & 21 & 19 & 18 & 15 & 27 & 27 & 5 \\ 14 & 9 & 27 & 5 & 14 & 20 & 15 & 27 \end{bmatrix}$$

6. The newly formed matrix contains the Cipher-text -

$$\begin{bmatrix} -119 & -120 & -207 & -77 & -182 & -176 & -186 & -165 \\ 19 & 30 & 46 & 23 & 29 & 47 & 42 & 32 \\ 135 & 127 & 221 & 78 & 209 & 181 & 201 & 179 \end{bmatrix}$$

7. To decrypt the matrix back into Plain-text, multiply it by the inverse of the cipher -

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} * \begin{bmatrix} -119 & -120 & -207 & -77 & -182 & -176 & -186 & -165 \\ 19 & 30 & 46 & 23 & 29 & 47 & 42 & 32 \\ 135 & 127 & 221 & 78 & 209 & 181 & 201 & 179 \end{bmatrix}$$

$$\begin{bmatrix} 16 & 7 & 14 & 1 & 27 & 5 & 15 & 14 \\ 5 & 21 & 19 & 18 & 15 & 27 & 27 & 5 \\ 14 & 9 & 27 & 5 & 14 & 20 & 15 & 27 \end{bmatrix} \longrightarrow \begin{bmatrix} P & G & N & A & & E & O & N \\ E & U & S & R & O & & & E \\ N & I & & E & N & T & O & \end{bmatrix}$$

Which contains the Plain-text -

PENGUINS ARE ONE TO ONE

Application 2

Suppose we want to send the following message to our friend,

MEET TOMORROW.

For the security, we first code the alphabet as described in Application 1 above:

Thus, the code message is

MEET TOMORROW											
M	***E***	***E***	***T***	***T***	***O***	***M***	***O***	***R***	***R***	***O***	***W***
13	***5***	***5***	***20***	***20***	***15***	***13***	***15***	***18***	***18***	***15***	***23***

The sequence

13 5 5 20 20 15 13 15 18 18 15 23

is the original code message. To encrypt the original code message, we can apply a linear transformation to original code message. Let

$$L : R^3 \longrightarrow R^3, L(x) = Ax$$

where

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix}$$

Then, we break the original message into 4 vectors first,

$$\begin{bmatrix} 13 \\ 5 \\ 5 \end{bmatrix}, \begin{bmatrix} 20 \\ 20 \\ 15 \end{bmatrix}, \begin{bmatrix} 13 \\ 15 \\ 18 \end{bmatrix}, \begin{bmatrix} 18 \\ 15 \\ 23 \end{bmatrix},$$

and use the linear transformation to obtain the encrypted code message

$$L\left(\begin{bmatrix} 13 \\ 5 \\ 5 \end{bmatrix}\right) = A \begin{bmatrix} 13 \\ 5 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 13 \\ 5 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 38 \\ 28 \\ 15 \end{bmatrix},$$

$$L\left(\begin{bmatrix} 20 \\ 20 \\ 15 \end{bmatrix}\right) = A \begin{bmatrix} 20 \\ 20 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 20 \\ 20 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} 105 \\ 70 \\ 50 \end{bmatrix}$$

$$L\left(\begin{bmatrix} 13 \\ 15 \\ 18 \end{bmatrix}\right) = A \begin{bmatrix} 13 \\ 15 \\ 18 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 13 \\ 15 \\ 18 \end{bmatrix}$$

$$= \begin{bmatrix} 97 \\ 64 \\ 51 \end{bmatrix},$$

and

$$L\left(\begin{bmatrix} 18 \\ 15 \\ 23 \end{bmatrix}\right) = A \begin{bmatrix} 18 \\ 15 \\ 23 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 18 \\ 15 \\ 23 \end{bmatrix}$$

$$= \begin{bmatrix} 117 \\ 79 \\ 61 \end{bmatrix}.$$

Then, we can send the encrypted message code

28 15 105 70 50 97 64 51 117 79 61

Suppose our friend wants to encode the encrypted message code. Our friend can find ***the inverse matrix of A first,***

$$A^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix}$$

and then

$$A^{-1} \begin{bmatrix} 38 \\ 28 \\ 15 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 38 \\ 28 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} 13 \\ 5 \\ 5 \end{bmatrix},$$

$$A^{-1} \begin{bmatrix} 105 \\ 70 \\ 50 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 105 \\ 70 \\ 50 \end{bmatrix} = \begin{bmatrix} 20 \\ 20 \\ 15 \end{bmatrix},$$

$$A^{-1} \begin{bmatrix} 97 \\ 64 \\ 51 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 97 \\ 64 \\ 51 \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \\ 18 \end{bmatrix}$$

and

$$A^{-1}\begin{bmatrix}117\\79\\61\end{bmatrix}=\begin{bmatrix}0&1&-1\\2&-2&-1\\-1&1&1\end{bmatrix}\begin{bmatrix}117\\79\\61\end{bmatrix}=\begin{bmatrix}18\\15\\23\end{bmatrix}$$

Thus, our friend can find the original message code

13 5 5 20 20 15 13 15 18 18 15 23

via the inverse matrix of A.

Similarly, if we receive the following message code from our friend

77 54 38 71 49 29 68 51 33 76 48 40 86 53 52

and we know the message from our friend transformed by the same linear transformation

$$L:R^3\to R^3,\ \ L(x)=Ax=\begin{bmatrix}1&2&3\\1&1&2\\0&1&2\end{bmatrix}x.$$

Thus, we first break the message into 5 vectors,

$$\begin{bmatrix}77\\54\\38\end{bmatrix},\ \begin{bmatrix}71\\49\\29\end{bmatrix},\ \begin{bmatrix}68\\51\\33\end{bmatrix},\ \begin{bmatrix}76\\48\\40\end{bmatrix},\ \begin{bmatrix}86\\53\\52\end{bmatrix},$$

and then the original message code can be obtained by

$$A^{-1}\begin{bmatrix}77\\54\\38\end{bmatrix}=\begin{bmatrix}0&1&-1\\2&-2&-1\\-1&1&1\end{bmatrix}\begin{bmatrix}77\\54\\38\end{bmatrix}$$

$$=\begin{bmatrix}16\\8\\15\end{bmatrix},$$

$$A^{-1}\begin{bmatrix}71\\49\\29\end{bmatrix}=\begin{bmatrix}0&1&-1\\2&-2&-1\\-1&1&1\end{bmatrix}\begin{bmatrix}71\\49\\29\end{bmatrix}$$

$$=\begin{bmatrix}20\\15\\7\end{bmatrix},$$

$$A^{-1}\begin{bmatrix} 68 \\ 51 \\ 33 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 68 \\ 51 \\ 33 \end{bmatrix}$$

$$= \begin{bmatrix} 18 \\ 1 \\ 16 \end{bmatrix},$$

$$A^{-1}\begin{bmatrix} 76 \\ 48 \\ 40 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 76 \\ 48 \\ 40 \end{bmatrix}$$

$$= \begin{bmatrix} 8 \\ 16 \\ 12 \end{bmatrix},$$

and

$$A^{-1}\begin{bmatrix} 86 \\ 53 \\ 52 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & -1 \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 86 \\ 53 \\ 52 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 14 \\ 19 \end{bmatrix}.$$

Thus, the original message from our friend is

	16	*8*	*15*	*20*	*15*	*7*	*18*	*1*	*16*	*8*	*16*	*12*	*1*	*14*	*19*
	P	***H***	***O***	***T***	***O***	***G***	***R***	***A***	***P***	***H***	***P***	***L***	***A***	***N***	***S***

Conclusion

As we live in a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

References

DOGAN-DUNLAP, H. Linear Algebra Students Modes of Reasoning: Geometric Representations. Linear Algebra and Its Applications (LAA),432. pp. 2141-2159, 2010.

Lester S. Hill
CRYPTOGRAPHY IN AN ALGEBRAIC ALPHABET
The American Mathematical Monthly, Vol. 36, No. 6. (Jun. - Jul., 1929), pp. 306-312.

Obaida Mohammad Awad Al-Hazaimeh
A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA, International Journal of Computer Networks and Communications Vol.5, No.2, March 2013

Raja P. V K., Chakravarthy A. S. N., a cryptosystem based on Hilbert matrix using cipher block chaining mode, International Journal of Mathematics Trends and Technology, Issue 2011

Singh, Kirat Pal, and Shiwani Dod. Performance Improvement in MIPS Pipeline Processor based on FPGA. International Journal of Engineering Technology, Management and Applied Sciences 4.1 (2016): 57-64.

Sunitha K, Prashanth K.S.
Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm.
IOSR Journal of Computer Engineering
(IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5
(Jul. - Aug. 2013). pp. 64.

Wu T. M., Applied Mathematics and Computation,
International Journal of Industrial and Systems Engineering
Volume 169, Issue 2, 2005