BUSITEMA
UNIVERSITY
Pursuing Excellence

P.O. Box 236, Tororo, Uganda
Gen: +256 - 45 444 8838
Fax: +256 - 45 4436517
Email: info@adm.busitema.ac.ug

www.busitema.ac.ug

APPLICATIONS OF LINEAR ALGEBRA TO CRYPTOGRAPHY: A CASE STUDY OF BUSITEMA UNIVERSITY, FACULTY OF SCIENCE AND EDUCATION.

BY

AKETCH BECKY FAITH

BU/UP/2018/3357

beckyfaithaketch@gmail.com

Supervisor: Dr Rebecca Nalule Muhumuza

A RESEARCH PROJECT SUBMITTED TO THE DEPARTMENT OF MATHEMATICS IN THE PARTIAL FULFILLMENT FOR THE AWARD OF A BACHELOR DEGREE IN SCIENCE AND EDUCATION AT BUSITEMA UNIVERSITY

DECLARATION

I Aketch Becky faith declare that this research project is my original work and has never been presented to any institution of higher learning for any award.

Sign... Date..

Becky faith Aketch

APPROVAL

This dissertation has been submitted for approval of the university supervisor

Sign

………………………………..

Date

………………………………..

Dr Rebecca Nalulu Muhumuza

DEDICATION

This report is dedicated to my beloved parents Mr. Opendi Benedict and Mrs. Opendi Margret for their financial support and belief in me. Special thanks goes to my beloved brothers Opendi Ben and Kuju Abel Denis for their financial support as well my supervisor **Dr Rebecca Nalule Muhumuza**, my lecturers and course mates. It is through your love, support, guidance and encouragement that I have been in position to achieve this goal

ACKNOWLEDGEMENT

First, I thank the Almighty God for sustaining my life and seeing me through this course at the university. I would not have achieved all that I have done without His mercy, grace favour and provision.

I extend my sincere appreciation to my supervisor Dr. Rebecca Nalulu Muhumuza for her high level of devotion, patience, monitoring, and guidance that she has afforded to me right from the inception of this study to its conclusion without which this couldn’t be a success.

I feel overwhelmed with indebtedness to my family most especially my beloved brother Opendi Ben because if it wasn’t for his support all this wouldn’t be successful. Furthermore, I appreciate the effort of my siblings, relatives and friends for the love, support, guidance, encouragement and assistance during the course.

Finally, I would like to extend my gratitude to my fellow course mates and friends for their encouragement and support throughout my study at Busitema University.

Table of Contents

LIST OF FIGURERS

LIST OF TABLES

LIST OF ABBREVIATION AND ACRONYMS

M – Mega Hertz

n – Rows of the matrix

m - Column of the matrix

nxn - Non zero matrix

ATM - Automated machine

A^{-1} - Invertible matrix

Adj - adjoint

ABSTRACT

In the field of mathematics a little is known about the application of linear algebra by the students of Busitema university faculty of science of Education

The study has the aim to explore and learn the use and implementation of linear algebra in the simple form of cryptography in Busitema University faculty of science and Education

Cryptography can be defined as the process of keeping information hidden from the unintended parties but for only those with the key decoded the message. Also cryptography can be employed in many different ways of transforming readable data into unreadable form.

This field describes an activity built around one of the techniques to illustrate the application of linear algebra to cryptography.

This technique involves the encoding and decoding of messages where characters in the original message are assigned to the numerical value and the matrix must be inverted for easy decoding.

The method proposed   and its principle has great potential to be applied in other situations where the message needs to be exchanged confidentially.

The findings of the message was to develop an e- massing secrete coding theory which showed user friendly and confidentiality. And this can generate easy confidential flow through electronics and online interactions through the use of telephones, computers, iPods and other electronic devices

CHAPTER ONE

1.0 INTRODUCTION

Linear algebra is a stand out amongst the most critical fundament ranges in mathematical field. It is a subfield of mathematics that deals with matrices and operation on the data structures

This is due to the essential role it plays in the development of other subjects, given its unifying and generalizing nature which is powerful for resolving problems in different fields. Carlson and porter (1993)

Numerous geometric subjects are examined making utilization of ideas from linear algebra and the thought of a directive change with an arithmetical adaptation of geometric change. At long last a lot of present day unique variable based math constructs on linear algebra and regularly gives solid illustration of general though .Poole (2010)

linear algebra can be comprehended to mean anything that is straight or level for instance in the xy- plain you may be acclimated to portraying straight line as the arrangement of answers for a mathematic statement of structure $y = mx+b$, where the slant m and the y –capture b are constants that together depict the line. In the event that you have contemplated multivariate analytics, then you will have experienced planes. Living in there measurements with directions portrayed by triples (x, y, z) they can be depicted as the arrangement of answers for mathematical statements of answers for mathematical statements of the structure $ax+by+cz = d$ where a, b, c, d are constants that together focus the plain. Kolman, (1996)

And cryptography simply mean the process of keeping information safe by changing it into a format that the unintended recipients cannot understand and it consist of the plaintext which the normal text is written in any human understandable language, encryption is the process of converting normal data into readable form. Cipher text is the unreadable output of an encryption algorithm and decryption is the process of converting encoded data into its original form that is readable and understood by humans or computer.

Security is a very important aspect in our world today which demands the attention of all. It is an aspect that cryptography comes to play as a measure to enforce security of information passing from one medium to another, cryptography has been important in the domain of computer for a period of time and it was mainly for security but now it is important because it helps in the transmission of sensitive information. Cryptography transforms original message i.e. audio, text or video privately which makes it difficult for an intruder to discover its original meaning .therefore cryptography refers to the process of securing the data meant to be exchanged or communicated.

It's also a mathematical technique related to the safety of information such as confidentiality, data integrity, and authentication. Therefore cryptography plays major role in cellular communication such as e-commerce, computer, pay television, sending e-mails, ATM cards, mobile banking etc.

Cryptography helps in keeping secrete writing that gives ability to large approach to safeguard the information that is presented in the unreadable format. It's categorized into two forms that is symmetric and asymmetric. Symmetric is where both the sender and the receiver have the same key for encryption and decryption whereas asymmetric cryptography is where two different keys are used , one for encryption and another for decryption.

When using cryptography the sender first encrypts the message before it is transmitted through the network to the receiver who decrypts the message before it's stored in its original content. Therefore there should be emphasis on the students to apply linear algebra in order to ensure information confidentiality in the institution so to ensure proper communication flow.

The aim of the research is to provide students with the knowledge of being creative and the mind of being helpful to the community and the country at large.

1.1 BACKGROUND

In order to reveal the history of linear algebra, it is of great value to first determine what linear algebra is. Therefore this definition is not complete and comprehensive answer but rather abroad definition loosely wrapping itself around linear algebra. Different answers will be used so as to see the perspectives. Firstly linear algebra is the study of algebraic structure called vector space. It is also the study of linear sets of equations and their transformation properties. Linear algebra is a branch of mathematics charged with investigating the properties of finite dimensional vector spaces and linear mapping between such spaces. (Strang . (1993))

This report discusses the history of linear algebra as it relates with vector spaces, linear sets of equation and transformation. The proposal seeks to give a brief review of the history of linear algebra as its practical applications touching on the on the various topics used in agreement with it.

Around 4000years ago, the people of Babylon knew how to solve 2x2 systems of linear equations with two unknowns. around 200BC the Chinese published the nine chapters of the mathematical art ,"they displayed the ability to solve a 3x3 system of equation (perotti) the simple equation of ax+b=0 is an ancient equation worked on by people from all walks of life.

The emergence of the subject came from determinants, values connected to a square matrix studied by the founder of calculus, Leibnitz, in the late 17th century. Langrage came out with his work regarding langrage multipliers away to characterize the minima and maxima multivariate functions (Darkwing) more than 50 years later, Cramer presented his ideas of solving system of linear equations based on determinants more than 50 years after Leibnitz (Darkwing) interestingly enough, Cramer provided no proof for solving nxn system. As we see linear algebra has become relevant since the emergence of calculus even though it's foundational equation of cx+d=0 dates back centuries. Euler brought to light the idea that that a system of linear equation does not necessarily have to have a solution (perotti). He recognized the need for conditions to be placed upon unknown variables in order to find a solution.

The initial workup until this period mainly dealt with the concept of unique solutions and square matrices were the number of equations matched the number of unknowns. With the turn into the 19th century Gauss introduced a procedure to be used for solving a system of linear equation. His work dealt mainly with the linear equation and yet to bring in the idea of matrices and their notations. His effects dealt with equations of different numbers and variables as well as the traditional pre 19th century works of Euler, Leibnitz and Cremer. Gauss' work is now summed up in the term Gaussian elimination. This method uses concept of combining, swapping and multiplying rows with each other to eliminate variables from certain equations. After variables are determined, the student is then to use back substitution to help find the remaining unknown variables.

As mentioned before, Gauss work dealt much with solving linear equations themselves, initially but did not have as much to do with solving linear equations themselves initially but did not have as much to do with matrices. In order for matrix algebra to develop a proper notation or method of describing the process was necessary. Also vital to this process was a definition of matrix multiplications and the fact involving it. The introduction of matrix notation and the inversion of the word matrix were motivated by attempts to develop the right matrix the Latin word for womb as a name for an array of numbers. He used the Latin word for womb as the name of an array of numbers and used womb because he viewed a matrix as a generator of determinants Turker, (1993). The other part matrix multiplication or matrix algebra came from the work of Arthur calyley in 1855.

Calyley's defined matrix multiplication as, the matrix co-efficient for the composite transformation T1T2 is the product of the matrix for t2 times the matrix of T1 Turker (1993). His work dealing in the matrix multiplication culminated in his theorem, the cayley Hamilton theorem simply stated a square matrix satisfies its characteristics equation. Cayley's efforts were published into two papers, one in 1850 and the other in 1858. His work introduces the idea of the identity of a matrix as well as the inverse of a square matrix. He also did much to further the ongoing transformation of the use of matrices and symbolic algebra. He used the letter A to represent a matrix, something that had been very little before his works. His efforts were little organized outside of England until the 1880s. matrix at the end of the 19th century were heavily connected with physical issues and for mathematicians , more attention was given to vectors and they provide the mathematical elements .for a time, however interest in linear algebra slowed until the end of world war 11 brought on the development of computers . Now, instead of having to break down an enormous nxn matrix. Computers could quickly and accurately solve these systems of linear algebra. With the advancement of technology sing the methods of cayley Gauss, Leibnitz, Euler, and other determinants of linear algebra moved forward more quickly and more effective. Regardless of the technology though Gaussian elimination still proves to be the best way known to solve a system of linear equation Turker, (1993). The influence of linear algebra in mathematical world is spread wide because it provides an important base to many of the principles and practices. Some of the things linear algebra is used to solve systems of linear format, to find least square best fit linear to predict future outcomes or find trends and the use of the Fourier series expansion as a means to solve partial differential equations. Other more broad topics that are used for are to solve questions of energy in quantum mechanics. It is also used to create simple every day house hold games like Sudoku. It is because of these practical applications that linear algebra has spread so far and advanced. The key however it is to understand the history of linear algebra provides the basis of these applications.

Although linear algebra is a fairly new subject when compared to other mathematical practices, its uses are widespread. With the efforts of calculus savvy Leibnitz the concept of using systems of linear equations to solve unknowns and formalized. Other efforts from scholars like cayley, Euler, Sylvester and others changed linear system into the use of matrices to represent them. Gauss bought the theory to solve systems of equations proving to be the most effective basis for solving unknowns. Technology continues to push the use further and further but the history of linear algebra continues to provide the foundation. Even though every few years companies update the textbooks, the fundamentals stay the same

1.2 STATEMENT OF THE PROBLEM.

In the world today a lot of sensitive information is being shared and transmitted amongst people and organizations through electronic devices and advanced technologies, this therefore requires enhanced security in passing information which can be solved by the application of cryptography. These deals with encryption and decryption of electronic data, promoting secure transmission of information electronically will help computer users in using electronic devices like smart phones, computer and so many others in securing their communication.

However when implementing cryptographic algorithm such as symmetric ciphers for example using random number generation which can easily be predicted causing information leakage hence killing security..

In response to these challenges, this study proposes to examine the inclusion of linear algebra to remove some of the above problems and enable passing secured sensitive information from one device to another.

1.3 MAIN OBJECTIVE

The main objective of this study is to explore and learn the use and implementation of linear algebra in the simple form of cryptography for example hill cipher by the computer science students of Busitema University

1.4 SPECIFIC OBJECTIVES

To impart the knowledge of applying linear algebra in the current problem of information exchange using linear transformation by computer science students of Busitema University.

To generate a simple numerical skill for sharing information by the computer science students in Busitema university.

1.5 RESEARCH QUESTIONS

What experiences can be attained by the computer science students of Busitema university faculty of education through the application of linear algebra in cryptograph.

In which way can sensitive information be passed on by the computer science students of Busitema university faculty of education with ease?

Which simplest method can be used by the computer science students of Busitema university faculty of faculty of education to exchange messages?

1.6 SIGNIFICANCE OF THE STUDY

There is several significance of this study that is to say the different findings of this study will bring a great impact to more researchers in order to understand the application of linear algebra in securing information exchange.

The study will identify the need of different mathematical ideas in contributing to understanding of different methods in which sensitive information can be passed from an individual to another with no difficulties for example with the aid of linear algebra hence mitigating the loss of sensitive information.

The study will provide opportunities of learning linear algebra with significant meaningful and challenging experiences which in turn will help in solving the problem faced in every day social life.

The study will help scholars and other researchers who will be interested in conducting research in the application of linear algebra and will be used as a secondary source of information by researchers will to further investigate on the topic.

1.7 THE SCOPE OF THE STUDY

The study will be conducted in Busitema university faculty of education in Nagongera along Tororo-busolwe road. The research will focus on the application of linear algebra to cryptography by the computer students. Transformation and number will be used in order to obtain the required data.

This system will focus on capturing the population that will welcome the use of cryptography through the application of linear algebra and the level at which electronic devices will be used to communicate through the interactions of sending messages.

1.8 THEORATICAL FRAME WORK

In Uganda, most institutions and organizations face numerous challenges in communicating; sharing sensitive information within and across the globe, this is due to limited knowledge about transformation in cryptography and its application in data security.

Theories and research carried out by numerous institutions and organizations indicate that there are few knowledgeable experts in the field of linear transformation in cryptography. This has however affected us in various ways such as social, economic and political spheres of life including data security and intelligence.

Therefore as a research student interested in overcoming these social challenges (data security and intelligence) I will use a research on linear transformation expression of lower and higher order non singular matrix and its application to frame work of this study.

The frame work therefore assumes that some students are not well versed with the application of linear transformation to cryptography which can enable the transmission of sensitive information from one person to another. This framework will focus on how students will impart the knowledge of linear transformation in the transmission of secrete messages which include the sender, receiver, message, and the feedback.

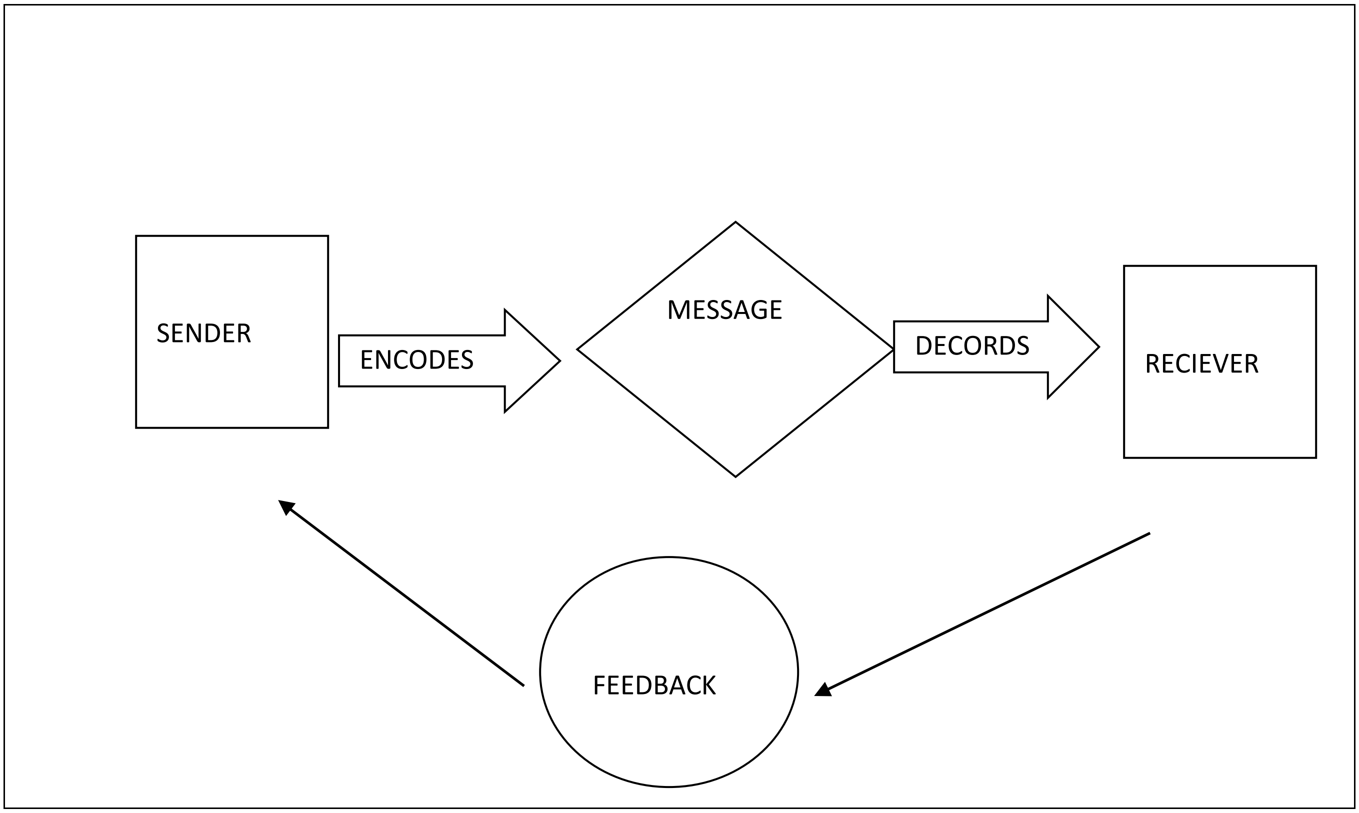
1.9 The key principles of cryptography are as follows

The sender encodes the message using the application of linear algebra (linear transformation) and the message is changed into matrix transformation and then it’s received by the receiver who decodes the message.

This enables us to ensure that the message encrypted contains redundancy that the intruder does not understand the message and it can be verified as fresh (not tampered).

An elaboration to show the flow of information which consist of the environment, sender, the message and the receiver

Figure 1: the key aspect in cryptography



When applying linear algebra (linear transformation) to cryptography, both the sender and the receiver should have understanding about linear transformation and the environment should also be favorable for the transmission of sensitive information (communication).

Since we are dealing with digital settings, the environment should be favorable so as to avoid intruders from accessing the message or the direction of the message

References

Tucker. (1993). *Linear Algebra.* Addison wesley company.

Howard Anton, Chris Romers(2005). *Elementary linear algebra with its application*

D. Grigoriev and V. Shpilrain, \Tropical cryptography," Communications in Algebra, Lester S. Hill, Cryptography

Laura smoller, l.(2012), january monday). *projects/cryptography material topics*. Retrieved fromedu.academia: https://www.projecttopics.org

Tucker. (1993). *Linear Algebra.* Addison wesley publishing company.

A.Menzes, P. O. *hand book of applied cryptography*. CRC Press, (1997.ww.projecttopics.org

JuYoung O.H et-al, "A Selective Encryption Algorithm based on AES for Medical Information," Health Informatics Research, Vol 16, No. 1, March 2010, pp. 22–29.

M.Zeghid et-al, "A Modified AES based Algorithm for Image Encryption," World Academy of Science, Engineering and Technology, 27 2007, pp 206 – 210.

Data Encryption Standard: http://csrc.nist.gov/publications/fips/fips 46-3/fips-46- 3.pdf

Advanced Encryption Standard: http://csrc.nist.gov/publications/fips/fips197/ fips-197.pdf

Xiaogang Jia et-al, "Image Encryption using IKEDA Map," International Conference on Intelligent Computing and Cognitive Informatics, IEEE Computer Society, pp. 455-458 , (2010)

Jose J. Amador, Robert W. Green, "Symmetric-Key Block Ciphers for Image and Text Cryptography," International Journal of Imaging System Technology, Vol. 15 – pp. 178-188, (2005).

Dragos Trinca, "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward Future Directions in Cryptography," Proceedings of The third International

Conference on Information Technology-New Generations. (ITNG'06), 0-7695-2497- 4 / 2006, IEEE Computer Society, (2006).

Adam J. Elbert, Christof Paar "An Instruction- Level Distributed Processor for Symmetric-Key Cryptography," IEEE Transactions on Parallel and distributed Systems, Vol. 16, No. 5, May, (2005).

Paul A.J., Varghese Paul, P. Mythili "Fast Symmetric Cryptography Using Key and Data based Masking Operations," International Journal of Computational Intelligence-Research and Applications. Vol. 3, No. 1, January-June 2009, pp 5–10.

Krishnamoorthy G.N, V. Ramaswamy, "Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images," International Journal of Network Security & its Applications, Vol.1, No.1, April 2009, pp. 28-33.

Camp, D. R. (1985). Secret codes with matrices. Mathematics Teacher, 78(9), 676–680.

Lee, P. Y. (2005). Teaching Secondary School Mathematics: A Resource Book. Singapore: McGraw Hill.

Singh, S. (1999). The Code Book: The Secret History of Codes and Code-Breaking. London: Fourth Estate.

http://www. richland.edu / James /lecture /.../matrices/applications.html

http://aix1.uottawa.ca/~jkhoury/cryptography.htm

Vasta B.S., Vasta Suchi.., Theoryof Matrices., Third edition. New Age International, India. 2010.

www.synopsys.com. C.J.R.Berges,

A.Menzes, P.Van Oorschot and S.Vanstoe, Hand book of applied Cryptography, CRC Press, (1997).

S.Wolfram, Cryptography with cellular automata, in advances in Cryptography-Crypto 85, Spring-Verlaglecture notes in

Computer Science 218(1986), 429-432.

Koblitz, Algebraic aspects of Cryptography, Springer-Velag, Berlin Heidelberg, New York.

P.Shanmugam and C.Loganathan, Involuntory Matrix in Cryptography, IJRRAS, 6(4) (2011).

Murphy S. (1990). The cryptanalysis of FEAL-4 with 20 chosen plaintexts. Journal of Cryptology, 2(1), 145–154.

Moore, G. W. (2001). Cryptography mini-tutorial. Lecture notes University of Maryland School of Medicine. Retrieved from http://www. medparse.com.

Obi, G. M. M. (2000). A generalization of the RSA algorithm. Proceedings of Computer Association of Nigeria Conference Series, 11(1), 203 – 207.

Olaoye, B. (2011). ICT security training scholarship to university. A letter of Invitation.

Potdar, V., & Chang, E. (2004). Disguising text cryptography using image cryptography. International Network Conference. United Kingdom:
Plymouth.

Rudolf, D. (2000). Development and analysis of block cipher and DES system. Retrieved from http://www.cs.usask.ca.

Schneier, B. (1996). Applied cryptography. New York: John Wiley and Sons.

Schneier, B. (2003). Practice cryptography. New York: John Wiley and Sons.

Stallings, W. (2006). Cryptography and network security (4th ed.). Englewood (NJ): Prentice Hall.

Steven, W.S. (2007). The scientist and engineer’s guide to digital signal processing. California: Technical Publishing.

Stroud, K.A., and Dexter, J.B. (2007). Engineering mathematics (6th ed.). New York: Palgrave Macmillan.

Su, N., Zobel, R.N. & Iwu, F.O. (2003). Simulation in cryptographic protocol design and analysis. Proceedings of 15th European Simulation Symposium. University of Manchester, UK.

Talbot, J., & Welsh, D. (2006).Complexity and cryptography: An introduction New York: Cambridge University Press.

The Times of India. (2011). Retrieved from http://www.timesofindia. indiatimes.com.

Young, A., & Yung, M. (2004). Malicious cryptography- exposing crypto virology. New York: John Wiley & Sons.

Yusuf, M. A. (2007). Data security: Layered approach algorithm (Unpublished master's thesis). Abubakar Tafawa Balewa University, Bauchi, Nigeria.

Wang, H. (2002). Security architecture for the teamdee system (Unpublished master's thesis). Polytechnic Institution and State University, Virginia, USA.

Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. IEEE Transaction Information Theory, 36(1), 553–558.

William, H. C. (1982). A p+1 method of factoring. Mathematic of Computation, l39 (3), 225–234.

Goh, E. (2007). Encryption schemes from bilinear maps (Unpublished doctoral dissertation). USA: Stanford University.

Kahate, A. (2008). Cryptography and network security (2nd ed.). New Delhi: Tata McGraw Hill.

Kak, A. (2009). Classical encryption techniques. Lecture notes on "Computer and Network Security". Purdue University.

Kessler, G. C. (2010). Handbook on local area networks: An overview of cryptography. United Kingdom: Auerbach. Retrieved from http://www.
garykessler.net/library.

Koblitz, N. (1994). A course in number theory and cryptography (2nd ed.). Berlin: Springer Verlag.

Laudan, C. K., & Traver, C. G. (2004). E-commerce. Business. Technology. Society (2nd ed.). New York: Pearson Education.

Menezes, A., Ooschot, P.V., & Vanstone, S. (1996). Handbook of applied cryptography. New York: CRS

Darkwing.(n.d.).*A brief history of linear algebra and matrix theory*

C. Paar and J. Pelzl, \Understanding cryptography: a textbook for students

and practitioners". Springer Science & Business Media, 2009.

M. M. Rahman, T. K. Saha, and M. A.-A.Bhuiyan, \Implementation of RSA
algorithm for speech data encryption and decryption," International Journal