SYMMETRIC ENCRYPTION ALGORITHM FOR SECURING DATA IN WAJIR COUNTY ICT DEPARTMENT.

NUH BILLOW ALI

ICT-3-2586-18

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DIPLOMA IN INFORMATION TECHNOLOGY OF GRETSA UNIVERSITY

NOVEMBER 2019

Declaration

This research is my original work and has not been presented for award of Diploma in Information Technology or for any other similar purpose in any other institution.

Signature: ______________________________ Date: __________________________

Nuh Billow Ali

ICT-3-2586-18

Supervisor

This research has been submitted with my approval as University Supervisor.

Signature: ______________________________ Date: __________________________

Mr. Vincent Mbadu

School of Computing and Informatics

Gretsa University - Thika

Table of Contents

List of Tables

List of Figures

Abbreviations and Acronyms

AES – Advanced Encryption Standard

CPU – Central Processing Unit

DES – Data Encryption Standard

GHz – Gigahertz

HTTPS – Hypertext Transfer Protocol

ICT – Information Communication Technology

NIST – National Institute of Standards and Technology

NSA – National Security Agency

OR – Logical Operator

RAM – Random Access Memory

XOR – Exclusive OR

Operational Definition of Terms

Attacker – A person who attempts, or successfully manages to circumnavigate the security of a cryptographic system by finding a weakness in the code, cipher, cryptographic protocol or key management system.

Broken – The presence of published means to brute force attach a cipher in a computationally fast way.

Ciphertext – The result of encryption performed on plaintext using an algorithm called a cipher.

Cryptography –Secure information and communication techniques derived from mathematical calculations called algorithms to transform messages in ways that are hard to decipher.

Decryption – The process of converting ciphertext to plaintext.

Digital Signature – A digital code generated and authenticated by public key, which is attached to an electronically transmitted document to verify its contents and sender's identify.

Distributed – Being located on different networks but being able to communicate and coordinate actions by passing messages to and fro through a network.

Encryption – The process of converting plaintext into ciphertext.

Key – A string of bits used by a cryptographic algorithm to transform plaintext into ciphertext or vice versa.

Symmetric Key – An encryption key used by both the sender and receiver.

Abstract

Security has been a paramount necessity over the years for every faction of society. Over time, security has been enforced through different mechanisms including digitization. In today's world, virtually each and every organization stored their data in digital databases. In the past, it had been enforced using physical phenomenon. This research was focused on the use of symmetric key cryptography as used in data security. Information was collected using both primary and secondary data sources. Secondary data sources were used for the collection of experimental data that the researcher could not acquire from primary data sources due to limitation in research facilities. The statement of the problem was centered around cyber-attacks that had become more frequent over the recent times.

CHAPTER ONE: INTRODUCTION

1.1 Introduction

This chapter has covered encryption in detail and has expounded on its evolution and implementations. Noteworthy, the research has mainly focused on computer based cryptography and more specifically encryption algorithms. In this chapter, the research has covered the background of the study, research problem, conceptual framework and research questions, objectives of the study and its scope and limitations.

1.2 Background to the study

(Sangapu et al, 2015) noted that one of the essential aspects of communication was cryptography. Cryptography was defined as the art of writing or solving codes (Concise Oxford Dictionary, 2007). The definition brought to light referred to cryptography in its simple form of secret communication. In computing, cryptography has been defined severally by various authors including (Yehuda el al, 2007) who described it as the scientific study of techniques for securing digital information, transactions and distributed computations. In this sense cryptography is a science of using mathematics to encrypt and decrypt data, thus allowing the storage of sensitive information and transmission through networks.

A cryptographic algorithm, also known as a cipher is a mathematical function that is used for the purposes of encryption and decryption. For the algorithm to work, there has to be a combination of a word, number or phrase. The security of encrypted data has been designed to depend upon two factors; the strength of the cryptographic algorithm and the secrecy of the key used for encryption. The cryptographic algorithm, its key and the components that make it behave as is all are collected to become a cryptosystem. The key allows decryption of data without which it would be very difficult to do.

There are two mechanisms used for encryption. These are the asymmetric and symmetric cryptographic techniques. In asymmetric cryptography, there is one pair of keys. One key is used for encryption while the other used for decryption. In symmetric cryptography, there is only one key that is used for both encryption and decryption. Asymmetric cryptography is also known as public key cryptography while symmetric cryptography is also known as private key cryptography.

The process of cryptography involves the scrambling of text into ciphertext; a process known as encryption and the reversal of scrambled text to plain text also known as decryption. In the type of cryptography under scope, a single key is used for both the aforementioned tasks.

AES has been considered to be the current standard for secret key encryption. It was created by Belgian scientists who specialized in cryptography. These were Vincent Rijmen and Joan Daemen. Their innovation went ahead to replace the old standard which was known as the Data Encryption Standard. The algorithm was designed to use a combination of XOR operations, octet substitution and row and column rotations. The reason for its success was attributed to its simplicity and ability to run on a regular computer.

The AES garnered recognition in 1997, January 2nd when NIST held a contest for new encryption standards, as a result of inadequacies discovered to be with DES. In 1998, DES was cracked in a period of less than 72 hours by a specially made computer and it costed less than $250,000 dollars.

AES was adopted by many stakeholders in the security sector including NSA for the USA government. This only made it popular from then on. The government of USA approved the standard for the purposes of securing classified information.

AES was designed as block cipher that encrypted a 128-bit block of plaintext to a 128-bit block of ciphertext, or performed the reverse process. The key used for encryption and decryption could be a 128, 192 or 256-bit long key which had to be kept secret. The length of the key led to the naming of the encryption/decryption process as either AES-128, AES-192 or AES-256 respectively. The iterations used for each process were either 10, 12 or 14 respectively.

The Wajir County government was constituted in the year 2010 after the promulgation of the new Kenyan Constitution. This county government was constituted to run itself and an independent entity and with it, came departments that necessitated its day to day operations. The ICT department was constituted to deal with all the matters that regarded to the county government digital assets. The ICT department was mandated with implementing data security, access and organization as well as developing necessary system and implementing them.

1.3 Statement of the Research Problem

In recent times, there have been continuous sabotage attacks on the cyber front. These attacks having been getting bolder over the time as observed during the June 3rd 2019 Kenyan government websites hack that lead to disruption of services and defacement of these websites.

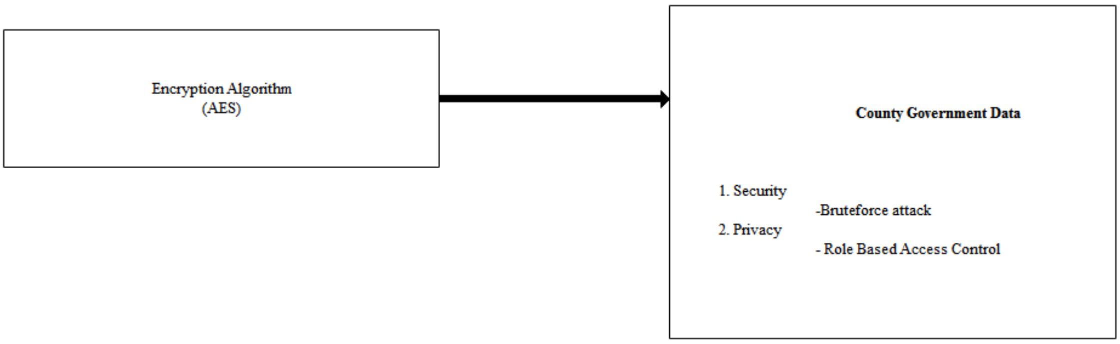
This meant access of data was determinant. Such attacks have spread to county governments and the need to protect data in the case of unauthorized access of areas storing such data was an eminent requirement. Unencrypted data stored in plain text could easily be accessed and used for purposes that could harm the operations of the county government as well as its employees and citizens. This has been known to happen when user data accessed is sold to highest bidders and used for purposes such as targeted marketing and further data compromise

1.4 Purpose of the Study

This study sought to find out the ways in which encryption standards, specifically the AES could be implemented in the county government in scope. The study also had the purpose of investigating the efficiency of the AES with regards to performance, and security. The study then sought to find out the current security measures that the county government in scope used to secure their digital data.

1.5 Conceptual Framework

Independent variable **Dependent Variables**



1.6 Objectives of the Study

1. To investigate the strengths of AES symmetric algorithm against brute force attacks.
2. To investigate the current security standards of the Wajir County government ICT deprtment.
3. To determine a practical implementation of the AES encryption algorithm for the county ICT department

1.7 Research Questions

1. What are the strengths of AES symmetric algorithm against brute force attacks?

2. What are the current security standards of the Wajir Count Government ICT Department?
3. What are the practical implementations of the AES encryption algorithm for Wajir county government ICT department

1.8 Significance of the Study

This study's significance has been rooted in security, especially data security. Cyber-attacks have been prevalent in recent times. These attacks have affected various people, organizations and governments alike. The investigation of ways that encryption standards could be used in the security of data shall benefit various players in the county government of Wajir, especially the ICT department which could be instrumental in implementation of the standards discussed. The study could also be useful to other players whose cyber security is in question including other county governments and organizations.

1.9 Scope of the Study

This study has been limited on two fronts. The first front is on the encryption standards investigated which fell under the category of symmetric encryption. The second front is focused on the ICT department of the county government of Wajir. This shall include personnel who interact with computers and security protocols used.

1.10 Limitations of the Study

These research limitations include:

1. Inadequate information through primary sources due to the technical nature of the subject.
2. Time constraints due to academic deadlines put in place.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature on the subject of the county government under scope and encryption as a cryptographic algorithm. The chapter has six sections each with a subject matter. Section 2.1 discusses previous work that has been published. It is broadened based on the research topic of this study. Section 2.3, 2.4 and 2.5 discuss the objectives of the study in detail and present literature that has already been done specific to these objectives.

2.2 Review of Related Literature

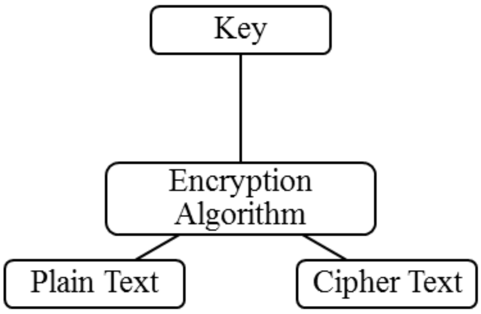
Cryptography implemented in the computer systems has been a fairly new topic that has lasted less than a century since its inception as observed in literature published over the years. (Katz, 2007) referred to this field of cryptography as modern, clearly distinguishing it from traditional cryptography. In the sections that follow the researcher has sequentially discussed the concepts that form the basis of it. The sections discussed are Cryptography being the foundation of all computer security and encryption standard AES.

Computer Cryptography

In the thesis proposal; Efficient Cryptographic Techniques for Securing Storage Systems, (Alina, 2007) noted that indeed cryptography has come to be applied in vast areas amongst them, storage security. (Alina, 2007) stated that it would have been inefficient for people to continue relying on servers to host and secure their data as had been tradition because they had become easier to compromise over time.

(Yehuda et al. 2007) defined modern cryptography as the scientific study of techniques for securing digital information, transactions and distributed computations. Modern day cryptography was advanced and involved systematic procedures to yield security by obscurity and the use of private keys was not fundamental anymore. Figure 2 has given a simple illustration of how cryptography works. Figure below shows the working of cryptography.

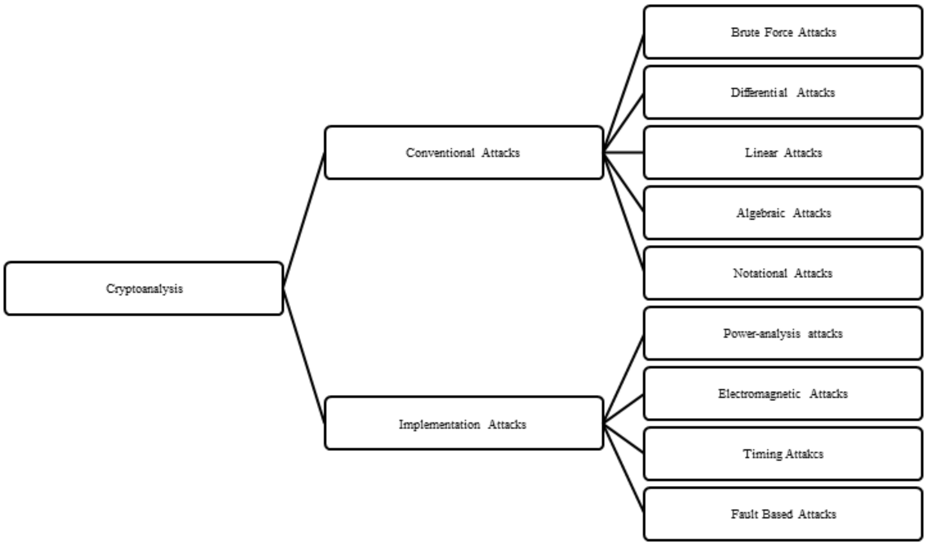
Figure 1: Simple Illustration of Cryptography



(Rosen, 2006) gave the fundamental objective of cryptography to be an enabler of two people communicating over an insecure channel to do so without an opponent understanding what was being said even if they intercepted the message.

(Jovanovic, 2015) in his thesis; Analysis and Design of Symmetric Cryptographic Algorithms illustrated various ways in which a cryptographic technique could be compromised. He stated that the success of any attack was measured in terms of required time, memory and data. Further (Jocanovic, 2015) stated that an attack was dependent on two factors; attack outcome and adversarial model. The adversarial model specified what an adversary was allowed or capable of doing during an attack. In an attack, the adversary was assumed to know all the cryptographic primitives save for the secret key, an assumption also known as the Kerckhoffs' Principle which was laid out by Auguste Kerckhoffs in his requirements for a usable cipher in 1883.

Figure 2: Attack Types Implementable in Cryptosystems



Advanced Encryption Standard

The basic mechanism used by the AES is derived from the cryptographic encryption basics. These basics include the taking of plain text through an encryption algorithm and generating cyphertext. The encryption process for AES was described as in the figure below by (Alexander Uskov, 2016).

Figure 3: AES encryption process

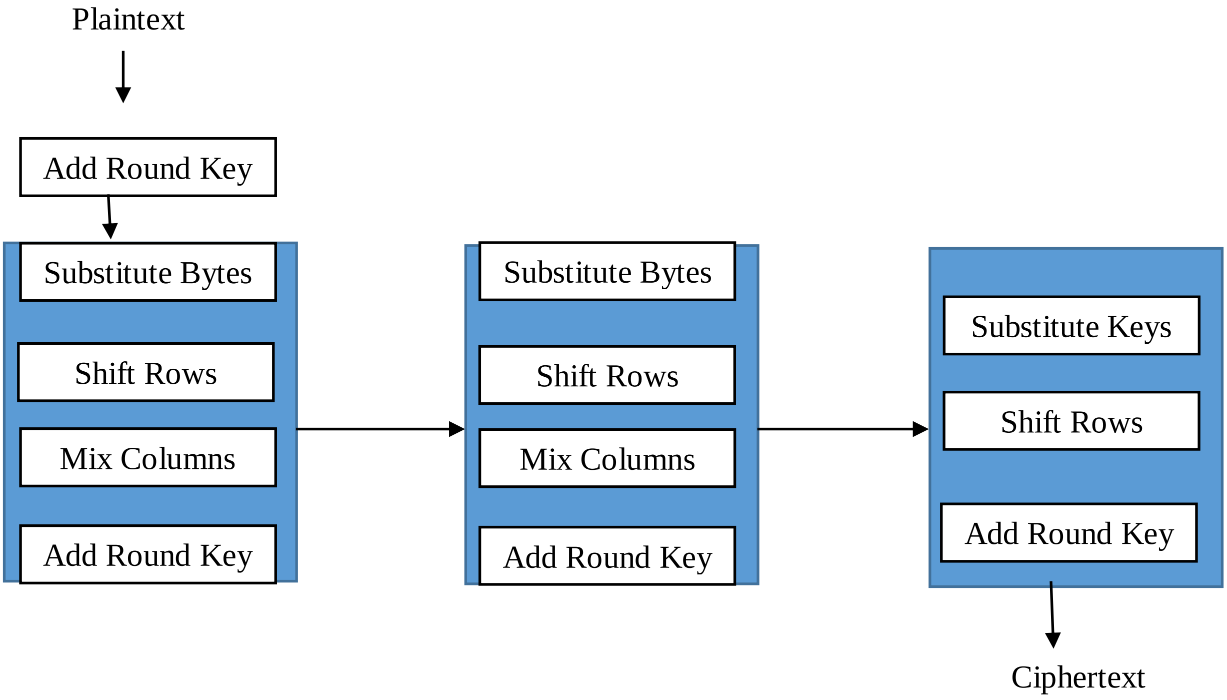
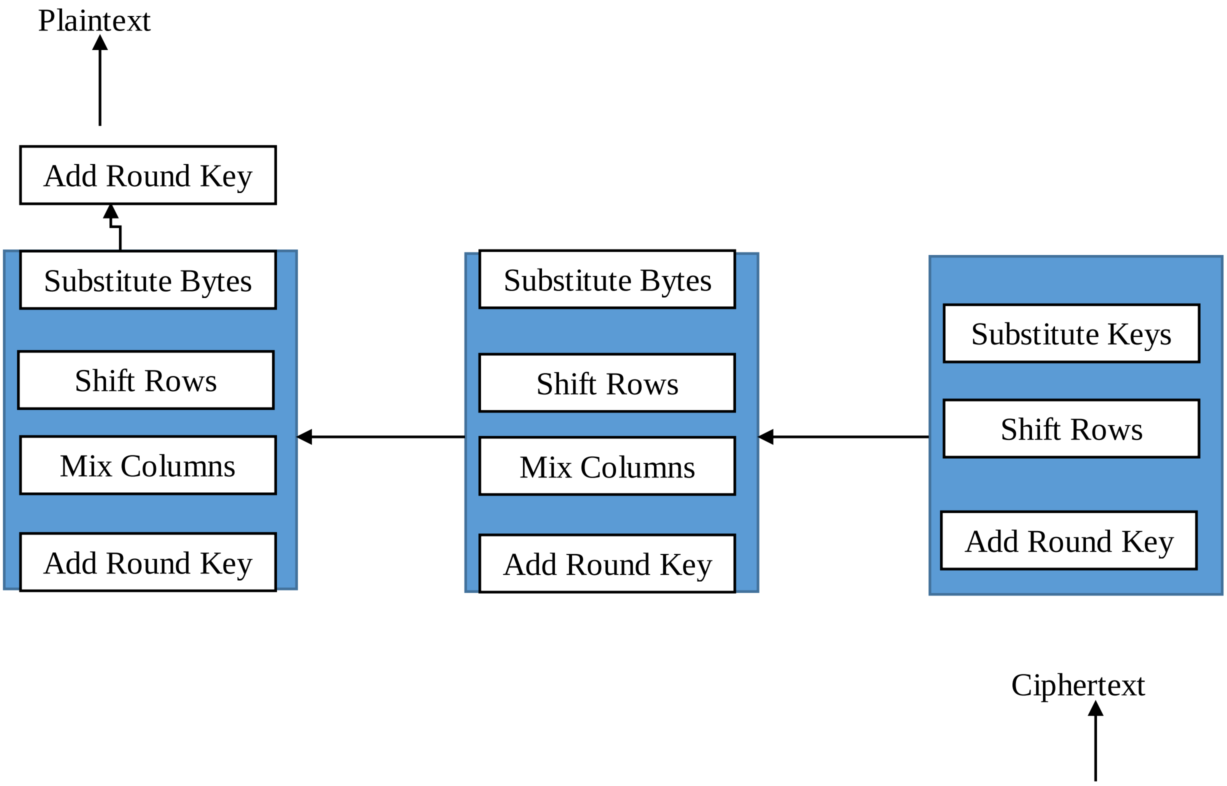


Figure 4: Decryption Process



2.3 Investigating Strengths of AES against brute force attacks

To investigate the strengths of AES, experiments had to be conducted to cover timing, security and other factors. In one such experiment, (Rashi et al, 2013) set up a lab for the experiment using a computer with a Core i3-2350M CPU @ 2.30GHz processor and varied file sizes varying from 355KB to 7.14MB were encrypted using the aforementioned CPU.

The experiment considered the time take to convert plaintext to ciphertext as encryption time. The importance of the encryption time was to calculate the speed of the encryption, thereby showing its efficiency. The throughput was equated to clock frequency of the CPU multiplied by 128 bits. The experiment further compared AES to DES and RC2. The conclusions to the research was that AES gave a higher throughput in comparison to the other encryption algorithms. This was however limited to the AES-128 encryption standard.

2.4 Theoretical Framework

Theories are formulated to explain, predict and understand phenomenon as well as challenge existing knowledge. The theoretical framework holds a theory of a research study, describing the theory that explains why the research system exists. It consists of concepts and together with their definitions and references to relevant scholarly literature. It must therefore demonstrate understanding of theories and concepts relevant to the topic. In the area of computer cryptography, not many theories have been put up. Most have been refined but still, the originals have stood the test of time. For the purpose of this research, one theory was identified and discussed to encompass the area of cryptography and hash functions in general.

Kerckhoffs' Principle

This theory posed a challenge to all cryptosystems identifying the requirements of any cryptosystem and the necessities when the systems was exposed to the public domain. (Kerckhoffs, 1883) stated that a cryptosystem should be secure even with everything about the system, except the key, is public knowledge. This concept has been borrowed to and implemented time and again in all cryptosystems that use asymmetric keys for encryption. According to Kerckhoffs, this cryptosystem should not have to be hidden from the general public in fact, the public should be aware of everything about the system but should not be able to break it. American mathematician (Claude, 1949) reformulated Kerckhoffs' principle but insisted that a system should be designed with the assumption that the enemy would immediately gain full familiarity with it. In this form, it was called the Shannon's maxim.

In his paper; La Cryptographie Militaire, (Kerckhoffs, 1883) stated six designs for military ciphers. The first was that the system (crypto) had to be practically, if not mathematically indecipherable. The second principle was that the system did not have to require secrecy and it also did not have to be a problem in the case that it fell into enemy hands. He also added that it had to be possible to communicate and remember the keys without having to write notes and correspondents had to have the ability to change or modify it at will. The fourth principle was that it had to be applicable to telegraph communication. Also, it had to be portable not requiring several persons to handle or operate. The final principle was that the system had to be easy to use and should not be stressful to use or require users to know and comply with a long list of rules. With the advancement in technology, some of these rules became irrelevant but the rule that has been in force to date was the second rule; a cryptosystem should not require secrecy, and it should not be a problem if it falls into enemy hands.

This principle had been applied in virtually all contemporary encryption algorithms in modern cryptography. The availing of these cryptosystems to the public for analysis and continued advancement ensured them to be secure and thoroughly investigated. In this state of publicity, the security of the system had to lie in the complexity of the algorithm itself, rather than secrecy. This had been applied widely in communication protocols such as HTTPS, SSL and TLS. To enforce the use of asymmetric algorithm, keys in internet communication could be generated randomly by the browsers and the servers. Knowing that there had been no perfect system, the integrity of the encrypted messages would eventually lie in the security of the private keys. The designers had to keep the designs at their optimum factoring in the worst case scenario where secured information has been fully disclosed. That factored in, the encryption algorithm had to be strong enough to stand as its last line of defence.

2.5 Summary of identified gaps in literature

The study identified that there was a lot of deficiencies when it came to the coverage of security within the county government under scope. This made it difficult to acquire data with regard to the aforementioned subject.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

(C.R. Kothari, 2004) defined research as a scientific and systematic search for pertinent information on a specific topic. Further, research had been described to be an original contribution to the existing stock of knowledge making for its advancement. Research Methodology was defined as the science of studying how research was done scientifically (C.R. Kothari, 2004). This chapter has been based on the aforementioned descriptions and in it the topics discussed have been ordered sequentially to fall under the broad categories of pre-data collection, data collection and post-data collection. In the pre-data collection category (3.1 – 3.9), the best mechanisms of how data is to be collected are discussed in section 3.10. Data has been analysed in the sections that follow.

3.2 Research Design

Research design is the arrangement of conditions for collections and analysis of data in a manner that aims to combine relevance to the research purpose with economy and procedure. (C.R Kothari, 2004). The research design therefore had the following importance;

1. Specification of the sources and types of information relevant to the research problem.
2. Strategy specifying which approach was to be used for gathering and analyzing the data.
3. Inclusion of the time and cost budgets.

The research design that was used for this study was the analytical research design that involved the use of fact-finding techniques which included research synthesis equipped to handle secondary data. Secondary data was preferred to primary data due to its ease in collection, low costs associated and the short period of time required for the collection. All these aided the researcher who had limited time and resources

The descriptive research design that involved the use of fact-finding techniques used to handle primary data. The use of primary data was necessary since the researcher endeavored to understand the concepts from the respondents who were affected. With this kind of data, many variables were uncontrollable by the researcher thus giving a further advantage for employing the aforementioned design. The researcher was compelled to only report the data as was collected.

3.3 Study Area

The study area that was considered for this study involved the Wajir County ICT department. This department is part of the large Wajir County located on the eastern part of Kenya. The study was localized to this specific department that was actively involved with the data security of the county government office. This included the ICT department which handled the servers storing the data.

3.4 Target Population

A target population is the entire group of individuals or objects to which a researcher would be interested in generalizing the conclusions. For this research, the researcher needed to acquire information on the efficiency of the encryption algorithm under scope as had been implemented over time. Acquiring expert advice from primary sources on the topic would prove to be a challenge during the research and as such, the researcher would intend to acquire the information needed for the study from researchers who had already published related data. Further information would be acquired from the personnel on less technical issues such as opinions and data security mechanisms used by the county government. The personnel targeted would be from the county’s ICT department.

3.5 Sampling Techniques

To ensure the efficiency of the information collected from secondary data, the researcher used one sampling technique. It was useful because the study topic was specific and needed a specific population to answer to the questions under consideration. The purposive sampling technique was used to identify the research papers that were most appropriate for collecting data related to this study. To ensure this was successful, the researcher first identified research papers that analysed results from experiment conducted to authenticate the research questions. This technique was also used to identify ICT personnel who would answer the questionnaire and give feedback as anticipated by the researcher.

3.6 Sample Size

A sample size has to be properly determined based on the expense of data collection and the need to have sufficient statistical power. It is an important feature of any empirical study with the goal of making inferences about a population from a sample. Sample size determination is the act of choosing the number of observations or replications to include in a statistical sample.

The researcher considered a sample size of 5 ICT personnel that were working in the county government of Wajir. This represented the whole technical ICT department.

3.7 Research Instruments

Research instruments are measurement tools designed to obtain data on a topic of interest from research subjects. The study highly relied on both secondary and primary data. To research on secondary data, the research used thesis that had been gathered from online sources relating to the AES. The researcher also used questionnaires as the instrument to collect primary data from respondents.

3.8 Validity of Measurements

This research could not ideally interfere with the variables under consideration. This meant that a research conducted would need to acquire measurements that were reasonable and sufficient in the consideration of the research topic. Research papers used were able to acquire data that was valid since it had been recorded through experiments that were done in controlled environment and with reliable hardware and software equipment. Further, the data acquired through the use of questionnaire came from actual persons who participated in the research. This meant that both the secondary and primary research instruments were valid.

3.9 Data Collection Techniques

The major data collection technique in this research was observation, for secondary data. This was the most reliable form of data collection for secondary data sources. Data was collected from several sources that had been collected during the sampling stage. Collection of data took the form of text that had been written. The primary data was collected using questionnaires and the responses from the respondents acted as the technique used for data collections.

3.10 Data Analysis

Once data had been collected, the researcher had to process the data into information and analyze it to come up with reasonable finding and recommendations. Processing in data research could be interpreted as editing, coding, classification and tabulation of collected data so that they would be amenable for analysis. Analysis implied to the computation of data along with searching of patterns of relationships that exist among data groups.

3.11 Logistical and Ethical Considerations

The logistical considerations were:

1. Risk mitigation – The researcher had to ensure that they could not in any pre-determinable way be exposed to cyber risk during the research because the research was conducted using internet resources.
2. Qualification of Research – The researcher had to know that the research papers analysed during the research could favourably answer the research questions, to the satisfaction of the research problem.
3. Data Collection – Observation of data collected had to be employed in this research to ensure data collected was effective to the research problem.

The ethical considerations were:

1. Plagiarism – This required the researcher to reference any non-original piece of text to the owner of the text as a way of academically respecting the works done by other researchers in the field.

CHAPTER FOUR: FINDINGS AND DISCUSSIONS

4.1 Introduction

This chapter discussed the findings of the research from both the secondary and primary data sources. The contents of this topic were organized into four sections including the overview of the findings, the discussion of the findings, critique of other studies and the inferences of the study. These were listed form section 4.2. to 4.5.

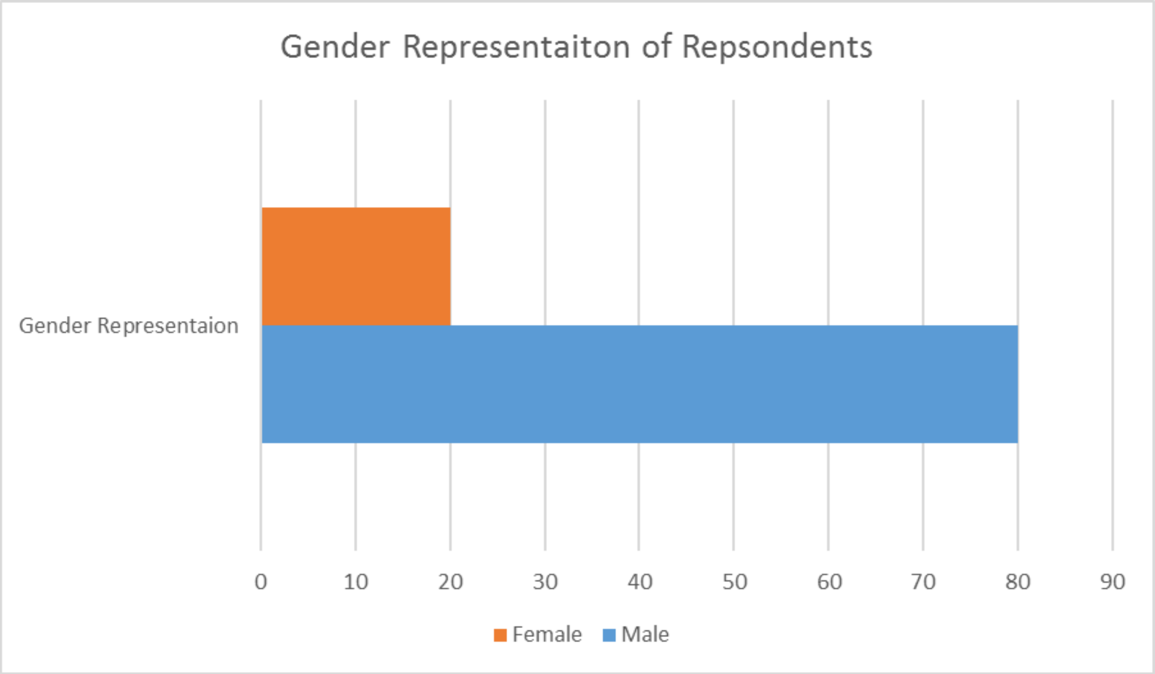
4.2 Overview of the Findings

The researcher used purposive sampling technique because he was aware of the persons who could take part in the research. These people were five and as a result, the researcher gave out five questionnaires. All the questionnaires were returned in a usable fashion. This was attributed the contained nature of the research. Table below represents these demographics.

Table 1: Questionnaire Return Data

Query	**Returned**	**Usable**
What number of questionnaires was returned and usable?	5 (100%)	5(100%)

Of the respondents who took part in the study, the researcher found out that a majority of them were male. This was not a surprise since a majority of employees in the Information Communication Technology were male. In the study, the research found that 20% of all the respondents were female while 80% were male. This data was represented in the graph below.



Further, the study sought to determine the average duration the respondents had worked for the county government. In the data obtained, the researcher found that the average work time in years for the respondents was 2.2. This showed that the respondents not only had expertise in their work area, but they also understood the workings of the county government. This was good for the researcher in the collection of more detailed data. In the research, the data collected showed that 20% of the employees had worked for a maximum of one year,60% had worked for between one and three years and another 20% had worked for more than three years. This data was represented in the table below.

Table 2: Work Experience

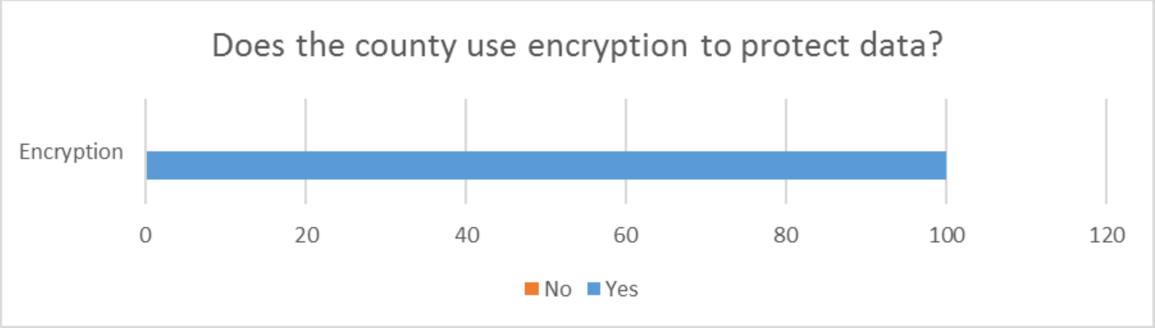
Years worked (Years)	**Number**	**Percentage**
0 – 1	1	20%
1 – 3	3	60%
More than 3	1	20%

In addition to the aforementioned queries, the researcher sough to find out if the respondents all worked for the anticipated departments. 100% of the respondents worked for the county government ICT department.

4.3 Discussion of the Findings

The first step in identifying the security standards used by the county involved finding out if the county government used any type of encryption on the data they stored in relation to their website. Encryption meant that the data store would not be accessed without a decryption key. The researcher found out that the county government did not encrypt their data using either symmetric or asymmetric encryption techniques. This was backed up by all the respondents. The graph below illustrates this.

Figure 5: Use of Encryption for Data Protection



If encryption was not in use, there had to be some other kind of security measure in place. The researcher noted in research that the use of passwords did not necessarily lead to encryption however, they could be used to allow log in into a system or deny it all the same. To do this, the system developer had to put in measures to ensure that data was not compromised in case an attacker was able to access the database. This could be achieved through the use of a hashing algorithm. This would abstract the real password in the database. The researcher sought to find out if the county had utilized any such security measure. The respondents noted that the implemented hashing algorithm was md5 which hashed all password stored in the database. This represented 100% of the respondents. The table below show information on the same concept.

Table 3: Hashing algorithm used

Query	**Algorithm**	**Respondent**
Which hashing algorithm do you use?	MD5	100%

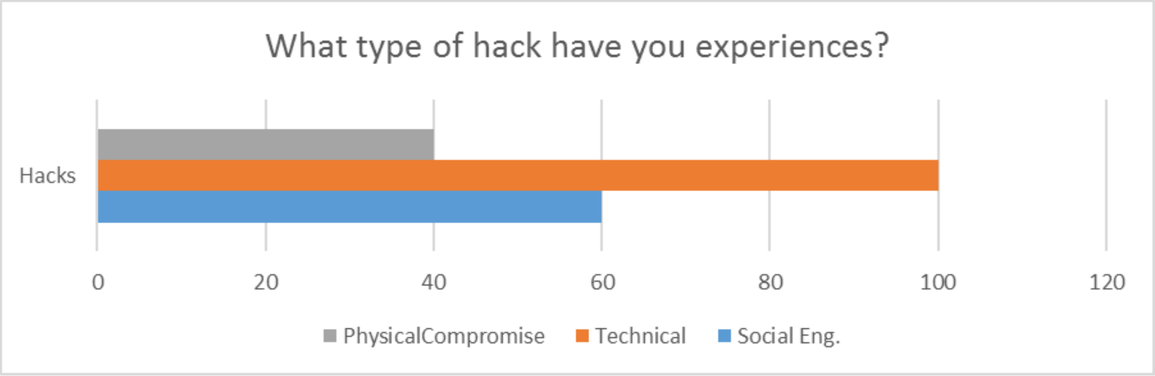
Another concept that was worth the research was the question on if any of the respondents had experienced hacking in the time working in the county government. The researcher noted that in their responses, the respondents acknowledged some form of hacking. The researcher had divided the hacking that could take place into three categories and queried the respondents on the same.

Table 4: Hacking Categories and Experiences

Hacking Category	Respondents	Percentage
Social Engineering	3	60%
Technical Hacks	5	100%
Physical Compromise	2	40%

The graph below represented the acquired information on the same topic on hacking.

Figure 6: Hacking Experiences



The final query posed for answer through the questionnaire as the primary mode of data collection was focused on the need by the county government to change their security measures. The query looked into whether the county government would want to upgrade their security mechanisms. The study found from the respondents that indeed the government would be interested in the same; being supported by all five respondents and representing 100%.

The second mode that the research used to collect data was the use of studies and archived that had been done with regard to the topic in question. For this, the researcher sought to identify the strengths of the recommended encryption technique, AES and its practical applications.

The characteristics of AES identified by (Dr.Prerna Mhajan et al, 2013) were represented in the table the follows. This kind of information was useful in understanding its usability in the real world.

Table 5: Characteristics of AES

Characteristic	**Value**
Key Size	128,192, 256 bits
Scalability	Not Scalable
Algorithm	Symmetric
Encryption & Decryption Key	Same
Power Consumption	Low
Security Level	Excellent
Deposit of Keys	Needed
Inherent Vulnerabilities	Brute Force Attack
Rounds	10,12, 14
Simulation Speed	Fast
Hardware & Software Implementation Fast	Fast
Ciphering & Deciphering Algorithm	Different

This data showed that AES could be implemented easily anywhere while providing the highest level of security. Further, AES was implementable through hardware and software, enabling use even in web systems.

In the study Comparison of Various Encryption Algorithms for Securing Data, (Dr. Kiramat Ullah et al, 2019) found out that AES was highly efficient. This was in comparison to other encryption algorithms including DES, IDEA, BLOWFISH and RSA. On a scale of 1 to 100, AES was found to rank at 90% efficiency while RSA followed with 65%, IDEA with 60%, BLOWFISH at 35% and DES at 30%. This information was represented in the table below.

Table 6: Efficiency of Encryption Algorithms

Algorithm	Efficiency in %
AES	90
RSA	65
IDEA	60
BLOWFISH	35
DES	30

4.4 Critique of Other Studies

The studies in scope were thorough enough in their data acquisition especially on experimental data. The researcher observed the use of labs set up to perform specific experiments. These labs contained computers with varied processors, RAM and storage capacity and type. In essence, it provided the researchers with a better shot at accuracy and diversity. In turn, other researchers who borrowed from the same studies inherited the same accuracy.

The studies that were observed during the research process lacked in the implementation of the encryption standards to county governments in Kenya. This caused an information gap that needed to be filled. Since most of the researches observed were experimental in nature, the result was data that did not factor in the human perspective or opinion.

4.5 Inferences of this Study

The use of encryption as a way of securing data was a proved method for data security. Symmetric encryption as designed relied on the safety of the decryption key. If the key was secure, AES became exponentially secure. Security of the encryption key relied on two factors; the strength of the key used and its safety with regards to being stolen.

The strength of the key involved the use of alphanumeric characters during the encryption process. If this key was easy for an attacker to guess, then the encryption would be vulnerable to brute force attack. If the key was complex, the encryption became exponentially strong.

Another note was with regard to the county government of Wajir. The county government was lacking in cyber security. This was proven through respondents' data that was collected during the research. As a result, there was immediate need to have the county government upgrade their security systems. This would not only safeguard their data but also prevent the loss of data through hacks and unauthorized access. The combination of encryption and hashing would suffice to provide this security.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter covered the conclusions, summary and recommendations for practice and further research. These sections were covered from section 5.2 to 5.5.

5.2 Summary

The pursued research had the aim of identifying the strengths of AES and its practical applications with regards to the county government of Wajir. The researcher realized that the acquisition of data from primary sources alone would not provide enough information to comprehensively cover the research topics. This lead to the use of both primary and secondary data sources as the means for research.

The researcher utilized two forms of research design. This was inherent of the fact that both primary and secondary data needed to be used. The descriptive research design that involved the use of fact-finding techniques used to handle primary data while t he analytical research design that involved the use of fact-finding techniques which included research synthesis equipped to handle secondary data.

The research coupled the research designs with purposive sampling technique was used to identify the research papers that were most appropriate for collecting data related to this study. To ensure this was successful, the researcher first identified research. This allowed the researcher to target specific research material in form of secondary data and identify personnel who would take part in the study with precision.

5.3 Conclusions

From the data collected, the researcher found that AES efficient for use with regards to any organization, government or personal need. It met all the requirements of a secure symmetric encryption algorithm. This was with regard to the continued growth in se of digital data and the advancement in cyber security compromises over the years. AES has been implemented in various areas and applied on a day to day basis due to its resistance to known attacks, simplicity and speed.

Due to the many factors considered for encryption algorithms and the factor of time being constrained due to academic deadlines, the researcher could not cover all the aspects in detail. This meant that there were still some areas that needed coverage.

5.4 Recommendations for Practice

Due to increased cyber-attacks, the need for higher security standards would be paramount. The researcher recommended the following for practice:

1. Adoption of encryption algorithms with higher security standards for the implementation of security such as AES.
2. The use of complex alphanumeric encryption keys during encryption to increase resistance against brute force attacks.
3. Encryption of data located on the servers to prevent data theft in case an attacker gained access to the database.
4. Hashing of passwords stored in online databases to avoid subsequent log in incase of data theft from the servers.
5. Adoption of AES by the county government of Wajir.

5.5 Recommendations for Further Research

Having noticed some deficiencies in the research covered, this study recommended the following:

1. Coverage of security measures implemented by other counties in Kenya.
2. Investigation into cyber security attacks that had happened and the best ways of defending against them.

3. Investigation into other encryption algorithms that could be implemented for data security in county governments.

REFERENCES

Alina Opera (2007). *Efficient Cryptographic Techniques for Secure Storage Systems.* CMU-CS-07-119. Carnegie Mellon University.

Bruce Schneier (1996). *Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C (Cloth)*. John Wiley & Sons, Inc.

C.R. Kothari (2004). *Research Methodology, Methods and Techniques.* Second Edition, New Age International Publishers.

Douglas R. Stinson (2006). *Cryptography Theory and Practice*. New York: Chapman & Hall/CRC.

Dr. Kiramat ullah, Bibi Ayisha, Farrukh Irfan, Inaam Illahi, Zeeshan Tahir. *Comparison of Various Encryption Algorithms for Securing Data.* Pakistan Institute of Engineering and Applied Sciences (PIEAS).

Dr. Prerna Mahajan & Abhishek Sachdeva (2013*). A Study of Encryption Algorithms AES, DES and RSA for Security*. Global Journal of Computer Science and Technology.

Jonathan Katz and Yehuda Lindel (2007). *Introduction to Modern Cryptography.* New York: CRC Press.

Philipp Jovanovic (2015). *Analysis and Design of Symmetric Cryptographic Algorithms.* University of Passau.

Rashmi R. Patil, Prof. V. V. Shete (2013). *Implementation of Advanced Encryption Standard on FPGA.* International Journal of Engineering Research & Technology (IJERT)

Douglas Selent (2010). Advanced Encryption Standard. Rivier Academic Journal, Volume 6, Number 2, Fall 2010.

APPENDICES

Questionnaire

My name is Nuh Billow Ali, a student at Gretsa University Thika. I am conducting an academic research into the security of county government data in order to recommend more secure and modern ways to achieve the same. The data collected here is for educational purposes only and shall be kept confidential.

Personal (Demographic) Questions

1. What is your gender? Male □ Female □
2. How long have you worked for the county government? ___________ Years
3. What department do you work in?

____

Technical Questions

4. Doe the county government use encryption for data stored on their online server?

Yes □ No □

5. If the answer to the previous question is yes; which encryption type do they use?

____

6. Does the county use hashing for passwords stored in their servers? Yes □ No □
7. If the answer to the previous question is yes, which hashing algorithm do they use?

____

8. Has your county government data been hacked? Yes □ No □
9. If the answer to the previous question is yes, what type of hacking occurred?
   Social Engineered □ Technical □ Physical Compromise □
10. Is the county government currently open to new security standards? Yes □ No □