**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE**

**BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSIC**

**RESEARCH PROJECT TITLE:**

**FILE ENCRYPTION TOOL**

**REGISTRATION NUMBER: CHERUIYOT PETER**

A research project Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Computer Security and Forensic Meru University of Science and Technology

**June, 2021**

# **DECLARATION**

I hereby declare that this report is my original work and has not been presented elsewhere for any academic certificate.

**CHERUIYOT PETER**

**CT206/0014/17**

**Sign: ………………………… Date: ……………………………**

The undersigned certify that they/he/she have/has read and hereby recommend for acceptance of Meru University of Science and Technology a Project Proposal entitled “File Encryption Tool”

**SUPERVISORS**

**J. MWITI**

**Sign: ………………………… Date: ……………………………**

**Designation, Department of Computer Science**

**Meru University of Science and Technology**

**P.O Box 972-60200, Meru, Kenya**

Table of Contents

[**DECLARATION** i](#_Toc93356421)

[**ACKNOWLEDGEMENTS** iv](#_Toc93356422)

[**Abstract** v](#_Toc93356423)

[**CHAPTER ONE** 1](#_Toc93356424)

[1.1 Overview 1](#_Toc93356425)

[1.2 Background of Study 1](#_Toc93356426)

[1.3 PROBLEM STATEMENT 2](#_Toc93356427)

[1.4 MAIN RESEARCH OBJECTIVE 2](#_Toc93356428)

[1.5 SPECIFIC RESEARCH OBJECTIVES 2](#_Toc93356429)

[1.6 SIGNIFICANCE OF THE STUDY 3](#_Toc93356430)

[1.7 SCOPE STUDY 3](#_Toc93356431)

[1.8 JUSTIFICATION OF THE SYSTEM 3](#_Toc93356432)

[1.9 LIMITATION 3](#_Toc93356433)

[DEFINITION OF TERMS 4](#_Toc93356434)

[**CHAPTER TWO: LITERATURE REVIEW** 5](#_Toc93356435)

[2.1 Introduction 5](#_Toc93356436)

[2.3 Cryptography Phases 5](#_Toc93356437)

[2.3 Types of Cryptography algorithms 6](#_Toc93356438)

[**2.3.1 Secret Key Cryptography (SKC) or Symmetric Encryption** 6](#_Toc93356439)

[**2.3.2 Public Key Cryptography (PKC) or Asymmetric Encryption** 7](#_Toc93356440)

[**2.3.3 Hash Functions** 8](#_Toc93356441)

[**2.3.4 RSA Algorithm** 9](#_Toc93356442)

[2.4 Cryptography Properties 10](#_Toc93356443)

[2.5 Choosing What to Encrypt 10](#_Toc93356444)

[2.6 Challenges of existing system 11](#_Toc93356445)

[2.7 Related Studies 11](#_Toc93356446)

[**CHAPTER THREE** 12](#_Toc93356447)

[METHODOLOGY 12](#_Toc93356448)

[3.0 Overview 12](#_Toc93356449)

[3.1 Agile Methodology 12](#_Toc93356450)

[**3.1.1 The agile model process flow*.*** 13](#_Toc93356451)

[3.2 REQUIREMENT GATHERING AND ANALYSIS: 15](#_Toc93356452)

[**3.2.1 METHODS OF COLLECTING DATA** 15](#_Toc93356453)

[3.3 Ethical considerations 15](#_Toc93356454)

[**CHAPTER FOUR: ANALYSIS AND DESIGN** 16](#_Toc93356455)

[4.0 Overview 16](#_Toc93356456)

[4.1Analysis of the Current System 16](#_Toc93356457)

[4.2 Feasibility study 16](#_Toc93356458)

[**4.2.1Technical Feasibility** 16](#_Toc93356459)

[**4.2.2 Social Feasibility** 17](#_Toc93356460)

[**4.2.3 Legal Feasibility** 17](#_Toc93356461)

[**4.2.4 Economic Feasibility** 17](#_Toc93356462)

[**CHAPTER FIVE: SYSTEM DESIGN AND IMPLEMENTATION** 22](#_Toc93356463)

[5.1 SYSTEM DESIGN 22](#_Toc93356464)

[5.2 SYSTEM CODING 23](#_Toc93356465)

[5.3 IMPLEMENTATION 24](#_Toc93356466)

[Challenges 28](#_Toc93356467)

[**CONCLUSION AND RECOMMENDATIONS** 28](#_Toc93356468)

[**Reference** 29](#_Toc93356469)

[**APPENDICES** 30](#_Toc93356470)

[Budget and Work Plan Development 30](#_Toc93356471)

# **ACKNOWLEDGEMENTS**

My greatest appreciation goes to the Almighty God who gave me the strength and hopes to carry out this project. I want to thank Meru University for granting me the opportunity to be part of the institution where learning has been an everyday experience for me. Special thanks to Mr. Jackson Mwiti my Project Lecturer and my supervisors, for his dedication, support and immense contribution academically in approving this project and being there to correct, suggest and support my ideas throughout the period of compilation.

My appreciation also goes to my family and friends for their financial, moral and motivational support. Without the support of anyone of them this project would not have been a reality. I

appreciate all of you. God Bless you all.

# **Abstract**

Cyber Security Plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about cyber security, the first thing that comes to our mind is ‘cyber crimes’ which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various cyber security is still a very big concern to many. This project mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. In a world reigned by speed and perfection, technology relies primarily on computer science. Be it a simple act of sending an email or a critical act of conveying billions of dollars, almost everything is merely a click away. The world of computer science keeps people engaged in activities like gaming, website surfing, social media, banking, digital citizenship etc. spanning its grip upon all domains like hardware, software, network, data etc. Because so many activities rely on computers, they attract criminals, which ultimately leads to cybercrime, which could be as elementary as a basic hacking or as elaborate as ransom-ware attacks or financial cybercrimes. The consequences may vary from loss of personal or sensitive information to loss of massive amount of money. Thus, the need for ensuring cybersecurity is paramount.

**List of Figures**

[Figure 1: Process of symmetric encryption 6](file:///C:\Users\Cheruiyot%20Peter\Desktop\Final%20Project\CHERUIYOT%20PETER%20Final1.docx#_Toc93354943)

[Figure 2 Process ofAsymmetric encryption 7](file:///C:\Users\Cheruiyot%20Peter\Desktop\Final%20Project\CHERUIYOT%20PETER%20Final1.docx#_Toc93354944)

[**Figure 3:Hash Functions Encryption** 8](file:///C:\Users\Cheruiyot%20Peter\Desktop\Final%20Project\CHERUIYOT%20PETER%20Final1.docx#_Toc93354945)

[**Figure 4 RSA Encrypion Process** 9](file:///C:\Users\Cheruiyot%20Peter\Desktop\Final%20Project\CHERUIYOT%20PETER%20Final1.docx#_Toc93354946)

[**Figure 5: Agile Model** 12](#_Toc93354947)

[Figure 6: Encryption Decryption Flowcharts 21](file:///C:\Users\Cheruiyot%20Peter\Desktop\Final%20Project\CHERUIYOT%20PETER%20Final1.docx#_Toc93354948)

[**Figure 7: File Encryptions Interface** 24](file:///C:\Users\Cheruiyot%20Peter\Desktop\Final%20Project\CHERUIYOT%20PETER%20Final1.docx#_Toc93354949)

**List of Tables**

[Table 1: Work plan development Table 30](#_Toc93355639)

[Table 2: Budget Plan Table 31](#_Toc93355640)

# **CHAPTER ONE**

## 1.1 Overview

This project be focus on file encryption tool which can encrypt file in their storage drives, since it is not safe to store files in a disk without encrypting them. Most of the users think that having a long password is enough to secure files and folders in their personal computers but it is not quite true, but not since internet is also a passage which hackers can access your machine.

## 1.2 Background of Study

Security is a system safeguards for protecting information technology against disasters, system failure, and an unauthorized access that can result in damage, loss or exposure of sensitive information. There are several reports of spammers, cybercrimes and hackers who break into people’s privacy to gain illegal access to their data according to McQuade et al, (2008). This has posed greater challenges on people who use database, online transactions and internet users. Information is a valuable and costly asset that must be presented, controlled and planned just like other valuable assets within an organization. This work is designed to provide a security mechanism using a computerized data encryption system, where readable data is altered into unreadable form to prevent unauthorized access. Encryption is able to use powerful computational mathematics concept to create coded message that is virtually impossible to break.

The art and science of keeping messages secure is called cryptography, and breaking cipher text is referred to as cryptanalysis. Encryption usually involves transforming information in plaintext using an algorithm to make it unreadable to anyone except those who possess encryption key. The output information is cypher text which can be reverse in process call decryption, as per Brown, et al, (2009, March).

However, the protection and privacy of data residing on our system is at most important file security issues induce protecting file from unauthorized access, protection can be accomplished at a number of levels at the lower level is user identification codes and password, at higher level are encryption techniques. In these mechanisms, file is systematically altered in such a way that if unauthorized users interrupt them, they will be unintelligible. File must be well managed and protected by organization and data centers network should ensures network security that accurate reliable transactions by guarding against unauthorized access to system files.

## 1.3 PROBLEM STATEMENT

Security has been day-to-day widespread and growing concern that affects all areas of the society, such that data and information security has become one of the most pressing challenges confronting all kinds of current organizations, owing to their rapid adoption of information technology (IT) entirety in their activities. This development has render data and information to more vulnerable to unauthorized users, spammers, crackers and hackers who break into people’s and organization’s privacy and gain access. This has no doubt posed greater challenges on people who use database, share files and other resources on computer networks.

However, Anderson, R. (1993, December) implies that the most challenging problem resulting from insecure file in a computer system and file sharing over networks can be due to improper security of files, unauthorized user can easily understand the content of plaintext file and plaintext files can be easily altered or modified by unauthorized person.

In most cases, file on transit can be easily tapped over communication channel (eavesdropping) by hackers or third party, modify posing threat to files hence need to improve on their security by encrypting them.

Although many encryption systems have been developed, they have had some setbacks such as the length of the secret key used, which is a major factor.

## 1.4 MAIN RESEARCH OBJECTIVE

The project main objective of this encryption tool system is to help the user to encrypt and decrypt file which they need to secure.

## 1.5 SPECIFIC RESEARCH OBJECTIVES

* Develop a system software that restrict unauthorized access to data files on systems.
* Enhance confidentiality by providing files protections from eavesdropping.
* Reduce stress, time consumption and cost of operation involved in a manual security system.

## 1.6 SIGNIFICANCE OF THE STUDY

This study serves as a contribution towards achieving Computer Security Goals (Confidentiality, Availability and Integrity) as well as improving information, data and information security on computerized information systems especially for organizations where data is transferred from one point to another. It contribute in solving the problems of insecurity on both network for individual computers on a network. It also enhances the ability to support customers by providing secured and accurate access to all information. In the same manner, it benefit those who transact online.

## 1.7 SCOPE STUDY

This work is only concerned with security of information (encryption and decryption) for firms and individuals. It does not consider the firms policies and other issues. The primary tools for security tools are cryptography which is used to hide files from public view or unauthorized persons and to ensure that integrity and privacy of any file sent across the network. Cryptography involves encryption and decryption process. The scope of this study entails files security, integrity, user authorization and key management of files using RSA.

## 1.8 JUSTIFICATION OF THE SYSTEM

With regards to existing system, it is important for organization to develop a new system tool. This system tool is designed with security as its watchword. It is able to check access to the system and provide improved system efficiency; the unintentional distortion of data be avoided and fraudulent practices and defaulters can be checked.

## 1.9 LIMITATION

Some of the limitations of this study is:

* Key distribution is the main limitation for the proposed file encryption system.

## DEFINITION OF TERMS

* Data: data is the raw fact or observation, typically about physical entity or business transactions. Technically, data is the raw form of information stored as columns and rows in our databases, network servers and personal computers.
* Cipher text: this is the encrypted data; it is also called a cipher.
* Decipher text: This is the decrypted data; it is also called a plain text.
* Data security: This is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data.
* Information: This refers to data that has been processed in such a way to be meaningful to the person who receives it.
* Cryptography: This is the science of scrambling data.
* Encryption: encryption is the conversion of data into a form that cannot be easily understood by an unauthorized people.
* Decryption: Decryption is the process of converting encrypted data back into its original form, so it can be understood.

# **CHAPTER TWO: LITERATURE REVIEW**

## 2.1 Introduction

This literature review explains concepts of the ways to find out all information that has been used to develop this system tool. Here, all the research that relate with this system has been analyzed (Okoli et al, (2010).

**2.2 Principles of Cryptography**

Cryptography is a science that studies how to protect the data privacy. It includes many ways to hide information in storage or transit. In addition, cryptography is associated with scrambling images and messages into cipher form (encryption process), then back again to its original form (decryption process). In other words, the encryption is the process to convert the readable information to non-readable data or cipher (Boneh et al., 2004).

In recent studies, cryptography is considered to be a mapping of both mathematics and computer science fields and it is disaffiliated closely with information theory, computer security, and engineering studies (Bibhudendra et al., 2007).

## 2.3 Cryptography Phases

Cryptosystems, in general, consists of two phases: The encryption phase that transforms the original secret data to the coded data, and the decryption phase that transforms back the encrypted data to the original secret data. The keys used in cryptosystems represent the strength of the encryption algorithm. These keys should be complex and large enough to achieve high security to the secret data. In addition to that, the implementation of the substitution and transposition operations provides enough complexity to produce more and more difficulties to prevent attackers from breaking the encrypted data.

This technique should eliminate the main problem in the existing encryption system that is the size of keys used is not large enough and the keys are less random (Lindner and Piker, 2011).

## 2.3 Types of Cryptography algorithms

The cryptography algorithms can be categorized into three categories based on the number of keys that are employed for encryption and decryption. The three types of cryptography algorithms are presented in the next sections.

### **2.3.1 Secret Key Cryptography (SKC) or Symmetric Encryption**

Symmetric encryption is the oldest and best-known technique. In this system, both the sender and receiver share a single key. This method is also called Secret Key Cryptography (SKC) because a single key is used for both encryption and decryption. A secret key, which can be a number, a word, or just a string of random letters, is applied to the original data to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet (Ahmad et al., 2015).

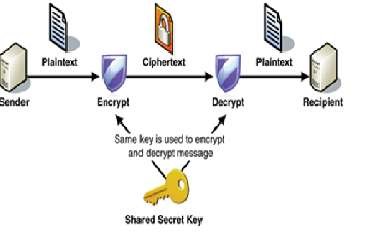
As long as both sender and recipient know the secret key, they can encrypt and decrypt all data using this key. An example of these types of cryptography algorithms are (DES, 3DES, AES,RSA, and RC4) (Delfs and Knebl, 2007). The process’s steps are shown in F

Figure 1: Process of symmetric encryption

**Figure 1: The process of symmetric encryption (Web Service Security, 2005).**

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

### **2.3.2 Public Key Cryptography (PKC) or Asymmetric Encryption**

**The asymmetric encryption uses two related keys-a key pair.**

A public key that is made freely available to anyone who might want to send you a message.

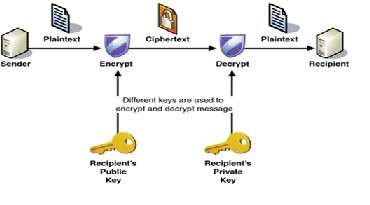
The second key is the private key. It is kept secret, so that only one person knows it. Any message (text, binary files, or documents) that is encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public).

Figure 2 Process ofAsymmetric encryption

Figure (2) illustrates the process of asymmetric encryption and asymmetric decryption (Web Service Security, 2005).

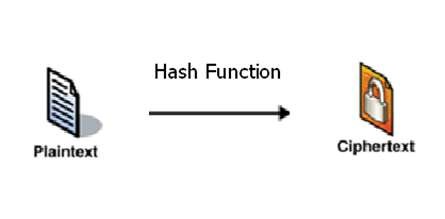
**Asymmetric encryption (Web Service Security, 2005).**

With asymmetric cryptography (also known as public key cryptography), the sender encrypts data with one key, and the recipient uses a different key to decrypt cipher text. The encryption key and its matching decryption key are often referred to as a public/private key pair. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. Examples of Asymmetric Encryption algorithms include (RSA, Daffier-Hellman, Digital Signature, ECDSA, and XTR).

### **2.3.3 Hash Functions**

Cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest or simply the digest (Kaur and Singh, 2012).

There are a number of hash functions types can be used in cryptography.

Two series of hash functions MD2, MD4, and MD5, and the Secure Hash Algorithm (SHA), a standard algorithm, that makes a larger (60-bit) message digest and is similar to MD4. These different types of hash functions have different features and shortages.

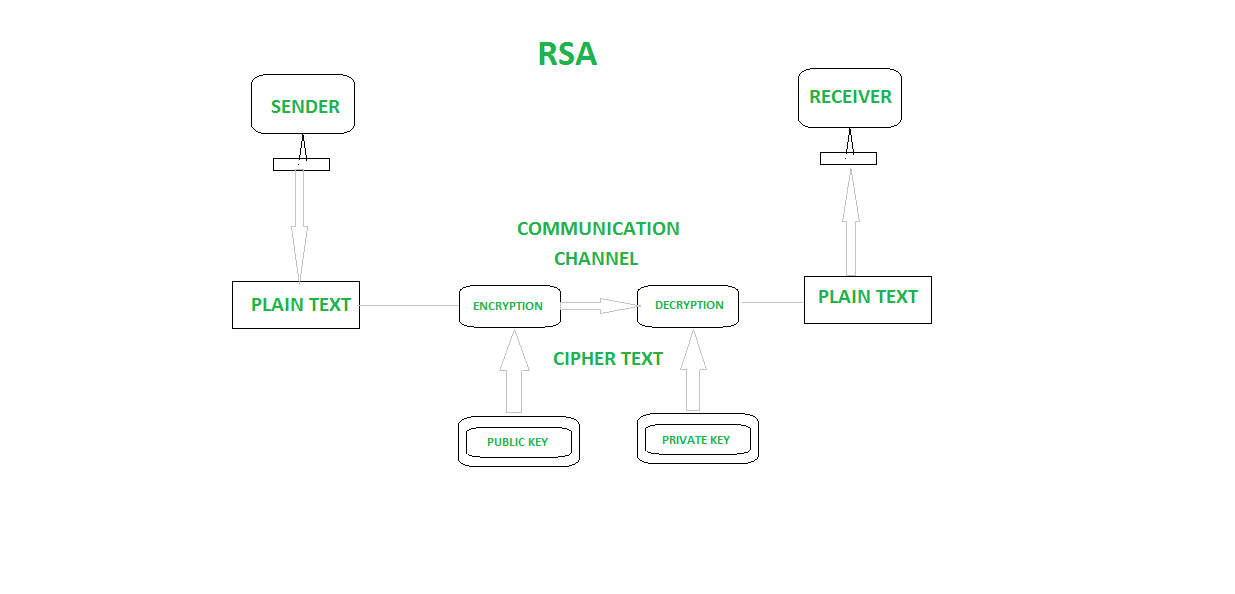
**Figure 3Hash Functions Encryption**

**Figure 3: Hash Functions Encryption** Common

**Hash algorithms include the following:**

* Message Digest (MD) algorithms: A series of byte-oriented algorithms that produces a 128-bit hash value from an arbitrary-length message.
* Secure Hash Algorithm (SHA): the SHA function is hash algorithm in which n-bit hash produces n-bit length finger print from the arbitrary length data. SHA- 1 produces message digest160, SHA-256, SHA-512, (Guo et al., 2010).

### **2.3.4 RSA Algorithm**

**** This is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

**Figure 4 RSA Encrypion Process**

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client’s public key and sends the encrypted data.
3. Client receives this data and decrypts it.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

## 2.4 Cryptography Properties

Cryptography provides a number of security properties to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography, it is widely used today. The most desirable property of any file cryptography is to maximize the strength of the secret key in order not to be hacked and to be secured against detection by unauthorized parties. The following sections show the various goals of cryptography (stalling fourth edition).

**Data Encryption Standard Algorithm** or **DES** is and algorithm develops as the official standard for secure transmission of data within the system. DES algorithm is a block encryption system that transforms 64-bits data blocks under a 56-bit secret key system.  The same algorithm and key are used for encryption and decryption, with minor differences. It converts the fixed length input data into encrypted data with the help of a few complex functions. This algorithm is commonly used in various applications like SSL.

## 2.5 Choosing What to Encrypt

Before enterprises can decide how to encrypt, they have to determine what to encrypt. Developing an encryption program should be part of an overall enterprise risk management and data governance planning process. Brotby, K. (2009) A comprehensive approach that considers specifically which data sets-structured, or unstructured- should be encrypted, and how key management should work will generate greater efficiency and effectiveness for an IT organization. There is no single universal standard for encrypting all data, on all systems, all the time. A successful approach will depend on the sensitivity and risk level of your organization’s information and its data storage methods. The first step is understanding the different types of encryptions, and what encryption can and cannot do.

**Three States of Data**

In order for data to be secure, it must be protected throughout its lifecycle. It is therefore important to consider the state of the data you are trying to protect:

1. **Data in motion:** being transmitted over a network

2. **Data at rest:** in your storage or on desktops, laptops, mobile phones, tablets and Iot devices

3. **data in use:** in the process of being generated, updated, erased, or viewed.

## 2.6 Challenges of existing system

An encrypting file system toolemploys secure and efficient mechanisms to encrypt or decrypt data on-the-fly as it is being written to or read from the underlying disk, to provide a level of data privacy that goes beyond simple access control. Also, issues such as trust models, backups and data recovery must be resolved. An encrypting file system must also be tightly integrated with the operating system for ease of use and flexibility.

Key management is one of the biggest challenges of building an enterprise encryption strategy because the keys to decrypt the cipher text have to be living somewhere in the environment, and attackers often have a pretty good idea of where to look.

Other challenges faced when designing a storage security framework include immunity from attacks launched by privileged entities, enabling legitimate remote access to shared encrypted volumes and providing a scalable and transparent key management scheme suitable for enterprise deployment.

Security in computing addresses these three goals. One of the challenges in building a secure system is finding the right balance among the goals, which often conflict. It is easy to preserve the particular objects confidentially in a secure system simply by preventing everyone from reading that object.

## 2.7 Related Studies

While much effort has been directed at securing network communications, security of stored data remains a largely neglected area both in the development and use of such systems. Nonetheless, various implementations of encrypting file systems exist. We first elaborate on some common design paradigms and then describe some popular related systems. The choice of the basic design approach greatly influences the security, performance and usability features provided by these systems.

File system level: Managing cryptography at the file subsystem layer of the operating system brings several advantages such as transparency to users and applications, flexibility of key management and access control, good performance, and immunity from an array of attacks. Separate keys may be used to protect different file system objects that may be shared with other users on an individual basis.

# **CHAPTER THREE**

## METHODOLOGY

## 3.0 Overview

This chapter outlines the methodology used in the study. It highlights the strategies that were used to conduct the study. It also includes the target of the study, sampling design, data collection and analysis and interpretation techniques. The idea of the proposed method is to encrypt file using some computational algorithms operations to produce a high secure encryption and decryption method. A set of successive keys are used in the transposition and substitution operations which adds significant protection to the input image. These keys are expected to increase the security of the proposed technique.

## 3.1 Agile Methodology

File Encryption system utilizes the agile model, this approach is unique from other approaches because the project can be broken into several phases. It involves constant collaboration with stakeholders and continuous improvement at every stage. Once the work begins, teams’ cycle through a process of planning, executing, and evaluating. Continuous collaboration is vital, both with team members and project stakeholders.



**Figure 5: Agile Model**

### **3.1.1 The agile model process flow*.***

1. **Conception** - At this stage the problem to be solved was perceived as the mode of File Encryption which enhances the security of file at large. The goal was identified after the problem is solved, estimating benefits in the new system over the current system, and identifying other areas that are affected by the solution.
2. **Inception** - Team members are identified whom includes the users, organizations/ company and the admin who is responsible for overseeing the system is working as it is designed to, funding is put in place, and initial environments and requirements are discussed. There are four objectives of the Inception phase that clarify the scope, project objectives, and feasibility of the intended solution:
3. Determine at least one possible solution. Assess whether the vision is technically feasible.
4. Understand what to build. Determine an overall vision, including the scope of the system and

its boundaries. Identify the stakeholders: who is interested in this system and what are theirr success criteria?

1. Identify key system functionality. Decisions of what is critical requirement will be determined for the platform to perform as required according to the above set objectives.
2. Understand the high-level estimates for cost, schedule, and risks associated with the project.
3. **Iteration/Construction** - The development team works to deliver working software based on iteration requirements and feedback. Multiple iterations will take place during the agile software development lifecycle and each follows its own workflow. During an iteration, it is important that the customers and business stakeholders provide feedback to ensure that the features meet their needs.

**A typical iteration process flow can be visualized as follows:**

* Requirements - Define the requirements for the iteration based on the product backlog, sprint
* backlog, customer and stakeholder feedback
* Development - Design and develop of the software will be based on defined requirements
* Testing - QA (Quality Assurance) testing, internal and external training, documentation
* development of the completed systems if it is performing as expected.
* Delivery - Integrate and deliver the working iteration into production
* Feedback - Accept customers’ and stakeholders’ feedback and work it into the requirements of the next iteration

1. **Release** - QA (Quality Assurance) testing, internal and external training, documentation development, and final release of the iteration into production. In agile software development a release is a deployable software package that is the culmination of several iterations. Releases can be made before the end of an iteration. This was applied in this project to ensure that the system was delivered as per the specification.
2. **Production** - Ongoing support of the software during all the stages of the development to its completion until it’s ready to deliver to its users.
3. **Retirement** - End-of-life activities, including customer notification and migration and the whole development process of this system will be officially brought to a close after the successful deployment of the application and the accompanying modules.

**ADVANTAGES OF AGILE METHODOLOGY.**

Customer satisfaction by rapid, continuous delivery of useful software.

1. Continuous attention to technical excellence and good design.
2. Regular adaptation to changing circumstrances.
3. People and interactions are emphasized rather than process and tools. Customers, developers and testers constantly interact with each other.
4. Working software is delivered frequently (weeks rather than months).
5. Close, daily cooperation between business people and developers.
6. Even late changes in requirements are welcomed

**DISADVANTAGES OF AGILE METHODOLOGY:**

1. Once we get proper requirements from client after showing prototype model, it may be of no use.
2. Agile is usually done at the cost of the developer. So, it should be done using minimal resources.
3. Too much involvement of client, is not always preferred by the developer.
4. Too many changes can disturb rhythm of the development team.

## 3.2 REQUIREMENT GATHERING AND ANALYSIS:

This is the phase where I gathered and analysed the entire requirement needed in the design of the Service Now system.

### **3.2.1 METHODS OF COLLECTING DATA**

***3.3.1.1 Observation***

This is the method where I visited the company physically and gathered information on how their support system operate. From the findings is when I got the requirements needed in redesigning a new system to automate their way of support. (Kawulich, B. B. (2005, May).

***3.3.1.2 Interview***

This is the method is used in speaking one on one with customers and staff to gather more data about their current system and the challenges they are facing and how best I can solve them by automating their processes. (Seidman, I (1998).) I used some designed questions to ask staffs and customers during the interview. Interviewing will help to collect data that are more accurate since the interviewees shall be involved in a one-to-one talk. This will give room to collect reliable data based on the system.

## 3.3 Ethical considerations

It is imperative that ethical issues are considered during the formulation of the evaluation plan. Ethical considerations during evaluation include:

# **CHAPTER FOUR: ANALYSIS AND DESIGN**

## 4.0 Overview

This chapter explain how the File Encryption Tools works with the aid of a data flow diagram. Functional and non-functional requirements are also mentioned in this chapter including method of how data is collected.

## 4.1Analysis of the Current System

## 4.2 Feasibility study

* This is a detailed study carried out whose purpose is to define the problem and decide whether or not a new system to replace the existing one is viable or feasible.
* The following are the areas of feasibility study:

1. Technical Feasibility
2. Social Feasibility
3. Economic Feasibility
4. Legal feasibility

### **4.2.1Technical Feasibility**

* Technical questions are those that deal with equipment and software e.g. determination of whether the new system can be developed using the current computer facilities. Since the system is web based, it only requires a computer with all the required developments environments e.g. sublime text editor, wamp/xampp for server and database hosting etc. Therefore, the system is technically viable.

### **4.2.2 Social Feasibility**

* This is also known as operational feasibility. It mostly deals with the effects of the system on the current society. The social feasibility is carried out along with technical feasibility such that the social implications of every alternative technical solution to the problem that emerges are evaluated. Socially, the system is not going to have much implication as it is a new system. User’s information especially in the registration interface will be put under confidentiality constraints. Therefore, no social threat shall be encompassed and the system is therefore socially viable

### **4.2.3 Legal Feasibility**

* The new systems legal implications are evaluated e.g.if it requires that the computer should be insured or whether the stored data should be registered with the government registrar before use. Every data that will be involved in this system will be true from competent sources and user’s data as well will be safeguarded against the confidentiality contract.

### **4.2.4 Economic Feasibility**

* Economic feasibility is aimed at determination of whether or not to continue with the project, depending on whether the project is economically viable. This system is within affordable budget limits since it is not very complex. Since all the required resources are at access with ease, the system will be economically viable.

**4.3. System Requirements**

System requirement are classified into two which include; functional and non-functional requirements.

**4.3.1 Functional Requirements**

Functional requirements explain what the system is required to do. The functional requirements of the current systems include;

1. The tool needs to access the file in the system.
2. Select the file to be encrypted.
3. Allow user to encrypt the file using RSA algorithms.
4. Encrypted file can be decrypted using the password used to encrypt.

**4.3.2 Non-functional Requirements**

On the other hand, non-function requirement provides a criterion that shows how the system performs a certain function.

The non-functional requirements include;

1. Security- the current tool ensures security by guarding the file against unauthorized access of computer files.
2. Reliability- The system allow user encrypt and decrypt files while instilling strong security measures.
3. Usability- the usability of the current tool is also convenient since one does not require too much skill to run the program.

**Encryption Decryption Process**

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

**Encryption Phase Algorithm**

The algorithm creates the encryption file from the source file; the following steps clarify in details the operations in this phase of the method.

**The encryption method has the following steps:**

**Step1:** Read (from the user) the secret key ***K*** of length

**Step2:** Read (from the user) the original file of length

**Step3:** Represent the original filenumber of blocks of size

To encrypt files or oder binary data, we use our own XOR encryption algorithm. Every bit (0/1) of the file gets with the bit of the hashed password into the XOR gate. See the explanations below:

Inputs Output

A B A XOR B

0 0 0

0 1 1

1 0 1

1 1 0

Original hash encrypted hash decrypted

0 XOR 1 = 1 XOR 1 = 0

1 XOR 1 = 0 XOR 1 = 1

0 XOR 0 = 0 XOR 0 = 0

1 XOR 0 = 1 XOR 0 = 1

A hash is a one-way function, that is a function, which is practically infeasible to invert. This program use this for two purposes:

1. To increase security

2. to make the XOR function easier.

Our hash algorithm is a slightly modified version of the sha512 hash algorithm.

To decrypt encrypted files we use the same function again: (encrypted) file XOR hashed password. It would take for decades to decrypt one encrypted file without the password or the hashed password. If you forget/lose your password, your files can't

be decrypted anymore.

**Decryption Phase Algorithm**

This algorithm will regenerate the source file from the encrypted file; the following steps clarify in details the operations in this phase of the method.

**The proposed decryption method has the following steps:**

**Step1:** Read (from the user) the secret key of length.

**Step2:** Read (from the user) the encrypted file of length.

**Step3:** Represent the file number of blocks of size

Decrypt file

Input Key

To Decrypt

Encrypt File

Encrypted File

Input Password to be hash(key)

Is RSA

Select file to Encrypt

No

Yes

Decrypted File

Figure 6: Encryption Decryption Flowcharts

# **CHAPTER** **FIVE: SYSTEM DESIGN AND IMPLEMENTATION**

## 5.1 SYSTEM DESIGN

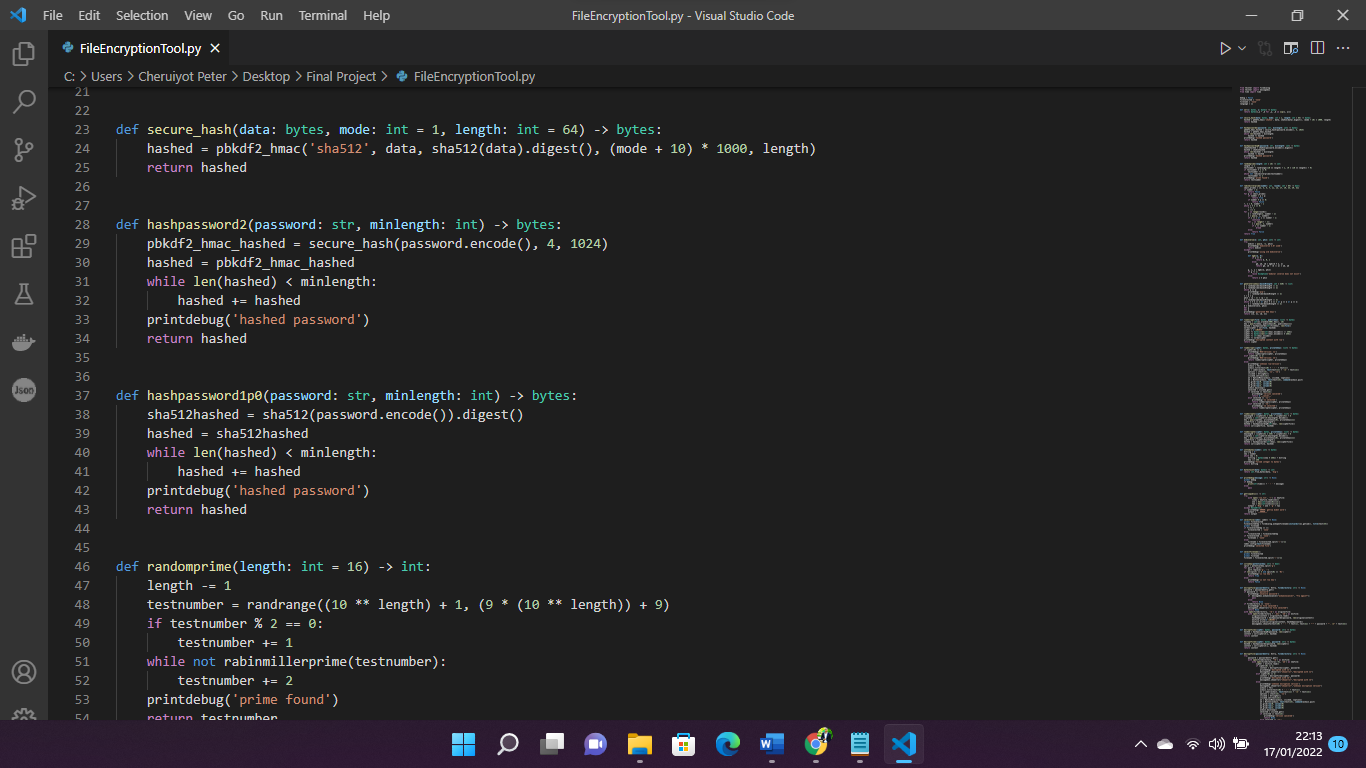
This is the process I used to define the elements of Service Now system such as the architecture, modules and components, the different interfaces of those components and the data that goes through that system. The requirement specifications from first phase are studied in this phase and system design is prepared. This helped me in specifying hardware and system requirements and helped in defining overall system architecture. To design the system, the following tools were used: Click charts for drawing the E-R Diagrams, Case Diagrams, DFD and Context Diagrams.

**Description of File Encryption Tool**

File encryption is one of the most effective security solutions. Combined with advanced security controls, it gives your business comprehensive data protection. File encryption tool is a system platform that uses encoding solutions to prevent unauthorized access to your files. In a world increasingly full of attacks and breaches, this tool is the key to keeping your data safe. File encryption works through the use of complex algorithms. An encrypted file is one that has had an encoding algorithm applied to it to scramble the data. The file becomes unreadable once scrambled, but the effect is only temporary. The encrypted data comes with a key the sender provides. This key usually takes the form of a password or passphrase, such as a string of alphanumeric digits, which enables decryption. Only individuals authorized to access the data receive the decryption key. Once the authorized recipient enters the correct password or passphrase, the file becomes readable again. Most operating systems and file systems have support for file encryption built in. The system safely stores sensitive files, and the decryption key provides access to them.

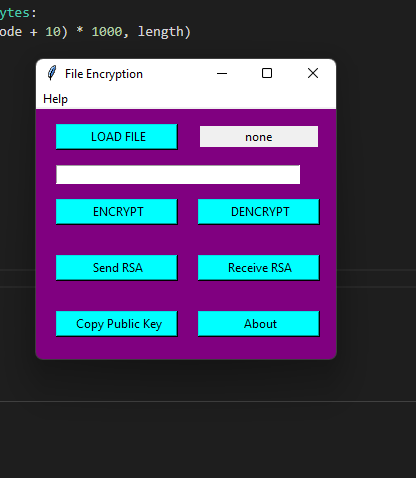
The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, then there's no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.

## 5.2 SYSTEM CODING

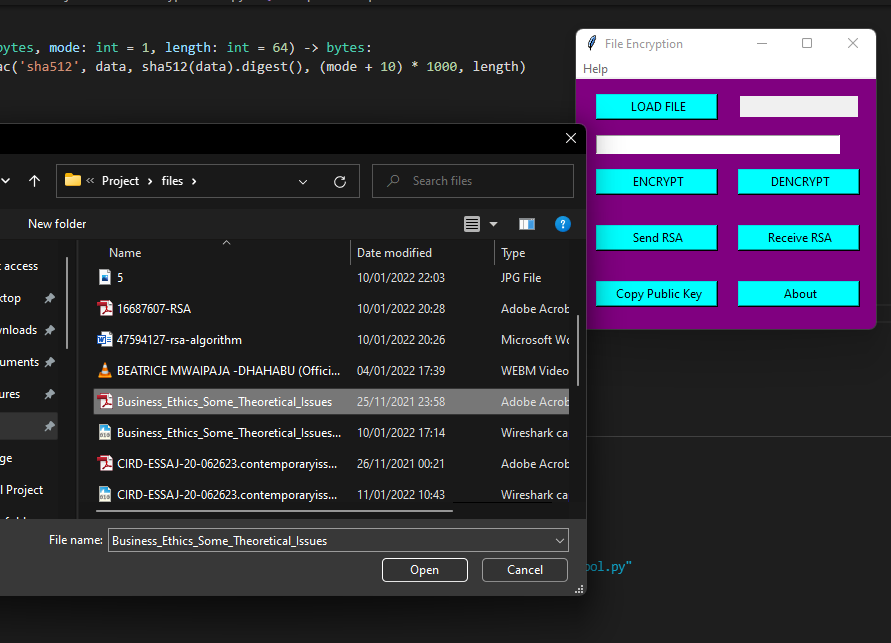
This is the process of writing system requirements into code. This is the actual stage of developing Service Now Help desk system it involves the process of converting the system into an executable system through writing lines of code and using the appropriate programming language and IDE. We have chosen Python as our programming language, because you can execute it on almost every operating system. Python is also easy to change if someone wants a new function. The only problem is, that on computers which haven't GNU/Linux or Python preinstalled, you need to first install the Python interpreter. For our other files, we've chosen txt as the file format, because it is readable with all operating systems.

## 5.3 IMPLEMENTATION

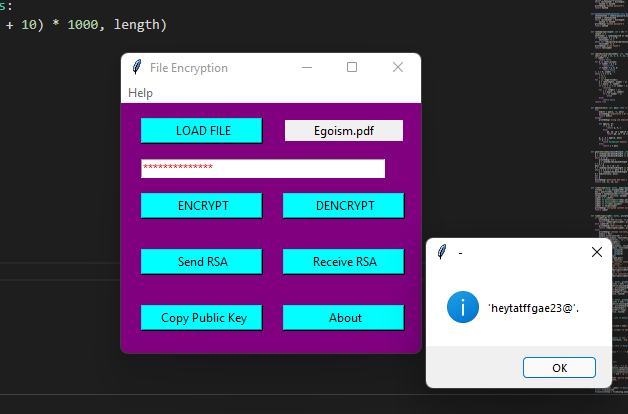
Implementation is the process of putting a decision or plan into effect. The system is first developed in small programs called units, which are integrated into the next phase. Each unit is developed depending on the requirements from the design phase once through it shall be tasted. The encryption and decryption algorithms has been implemented using Python. The experiments are done using different files that have different sizes.

To evaluate the encryption/decryption processes on the files, different files and different secret keys have been used.

**Figure 7: File Encryptions Interface**



Choose the file to Encrypt and enter your password ( You need to remember it to decrypt )



File

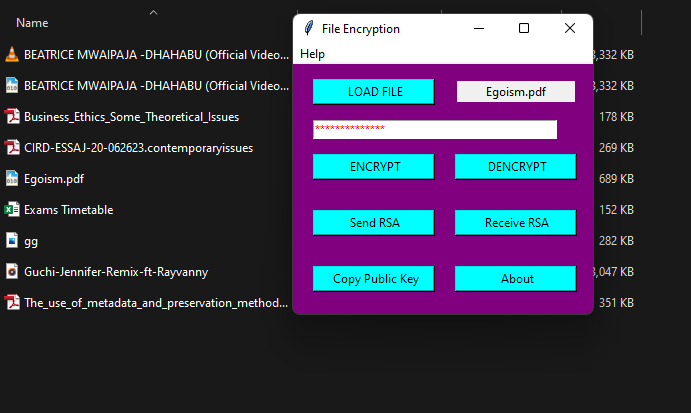
Enter

Password

Entered

Password

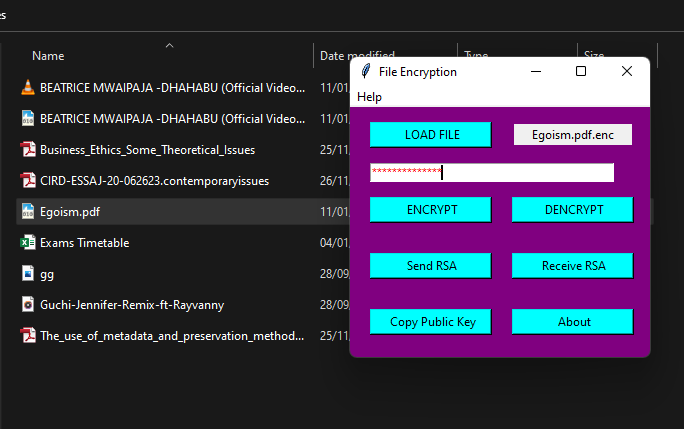
Enter password ( You need to remember it to decrypt )



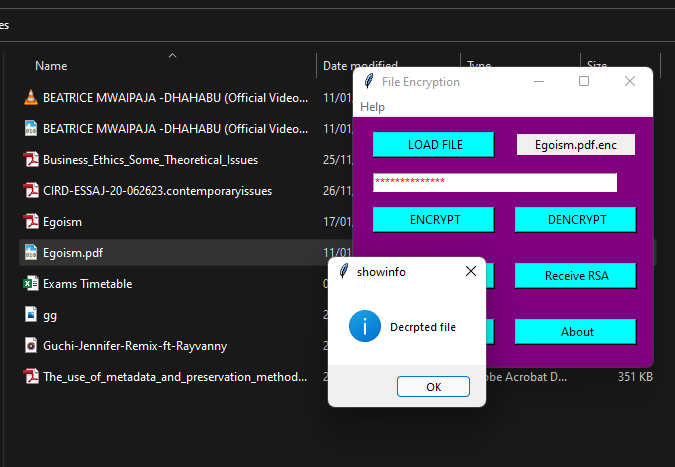
“Filename.enc” is created Encrypted File

**Decryptions Process**

When you need to Decrypt, load the file in the same way, enter the same password you have set while encrypting, you will find the decrypted file in the folder where your “.enc” file is kept.



Encrypted File

File successfully decrypted using encryption keys

Decrypted File

## Challenges

The most challenging thing with the tool was is loading a large files.System took longer time to encrypt and decrypt larges making the operations of encryption and decryptions process.

# **CONCLUSION AND RECOMMENDATIONS**

From observation the algorithm used, achieved good results in all experiments with a high security and less time. After, comparing the related work with this system, this technique is more reliable due to the long secret key and its complexity and randomness.

Due to the features of the algorithm technique some recommendations are suggested to be implemented such as: The ciphering method must be developed to include byte to byte encryption, and this method must be developed to be used in various applications such as whatsApp, twitter and other social media application.

# **Reference**

1. Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). Quantum cryptography. *Scientific American*, *267*(4), 50-57.
2. Guo, J., Ling, S., Rechberger, C., and Wang, H. (2010). Advanced meetin-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. In Advances in Cryptology-ASIACRYPT 2010, Springer Berlin Heidelberg, 56-75
3. Boneh, D. Di Crescenzo, G. Ostrovsky, R. and Persiano, G. (2004). Public key encryption with keyword search. In Advances in Cryptology-Eurocrypt. Springer Berlin Heidelberg, 506-522.
4. McQuade III, S. C. (Ed.). (2008). *Encyclopedia of cybercrime*. ABC-CLIO.
5. Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.
6. Delfs, H. and Knebl, H. (2007). Symmetric-key encryption Introduction to cryptography: principles and applications. Springer.
7. Anderson, R. (1993, December). Why cryptosystems fail. In Proceedings of the 1st ACM Conference on Computer and Communications Security (pp. 215-227).
8. Benoit, O., Dabbous, N., Gauteron, L., Girard, P., Handschuh, H., Naccache, D., ... & Whelan, C. (2004). Mobile Terminal Security. *IACR Cryptol. ePrint Arch.*, *2004*, 158.
9. *Lindner, R. and Peikert, C. (2011). Better key sizes (and attacks) for LWE-based encryption. In Topics in Cryptology–CT-RSA 2011, Springer Berlin Heidelberg, 319-339*
10. Brown, J. A., Houghten, S., & Ombuki-Berman, B. (2009, March). Genetic algorithm cryptanalysis of a substitution permutation network. In *2009 IEEE Symposium on Computational Intelligence in Cyber Security* (pp. 115-121). IEEE.
11. Charomie, A., & Wi, T. (2010). *Implementation of hybrid encryption method using Caesar'Cipher algorithm* (Doctoral dissertation, BSc. Thesis of Bachelor of Computer Science (Computer Systems & Networking), Faculty of Computer System & Software Engineering Universiti Malaysia Pahang (UMP)).
12. Brotby, K. (2009). *Information security governance: a practical development and implementation approach* (Vol. 53). John Wiley & Sons.
13. Durumeric, Z. (2017). *Fast internet-wide scanning: A new security perspective* (Doctoral dissertation).

# **APPENDICES**

## Budget and Work Plan Development

A work plan is a document that represent and specifies a justice reform program’s main activity, timing, their sequence and who will be responsible in each case. Work planning sets the stage for the system implementation.

In planning for the Consultant booking system, the development will take a maximum of four months. It is aimed to ensure every proposed objective of the system is well delivered. The work plan is broken down into the following manageable activities and respective timeline for each task.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | October | November | November/December | December |
| Data collection, analysis and requirement specifications |  |  |  |  |
| Design and prototyping |  |  |  |  |
| Frontend and backend development |  |  |  |  |
| Backend implementation, Testing, and delivered |  |  |  |  |

Table 1: Work plan development Table

A budget estimates the costs as accurately as possible for each activity set out in the work plan (Akramkhanov, 2019). It should distinguish between one-time costs, such as equipment purchase, and ongoing costs, such as operating expenses. Budgeting makes system implementation possible.

Budget

|  |  |  |
| --- | --- | --- |
| Budget Activity | Budget Amount in Ksh | Description |
| Travelling, Data collection, interviews | Ksh 3000 | This is the amount of money incurred in traveling for information gathering. |
| Hardware Resources | Ksh 50,000 | Amount of money to be spend in purchasing hardwares |
| System Development | Ksh 1000 | Development involves online engagement hence purchase of internet data bundles to facilitate communication, GitHub repository. |
| System Testing and hosting | Ksh 2500 | No expenses in terms of money in this phase. Testing will be done by the programmer and a few of the course mates. |

Table 2: Budget Plan Table