**INTRODUCTION**

Information security is the means of securing data or information from loss, theft, destruction, corruption and unauthorized access. In the past, security was simply a matter of locking the door or storing files in a locked filing cabinet or safe. Today, paper is no longer the only medium of choice for housing information. That information can also be stored in computer database, hard drives, floppy disks and other means of data storage. Therefore information security helps to ensure privacy and also protection of personal information.

One of the techniques of one of achieving this purpose is “Cryptography”. Cryptography is one of the most important tools for privacy and also a means of access control or restriction. Cryptography is one practical means of sending information over an insecure channel. These channels may be computer networks, telephone lines, wireless intercom system, internet, bank ATM etc.

**BACKGROUND**

According to Demmy (1989) data security simply means the act of protecting something against attack, security is done as a result of safety.

Security is a primary issue which means that staffs of Nigerian Police need to ensure that any confidential information is kept safe from corruption, destruction, theft and unauthorized access. Transmitting sensitive information such as security of financial data requires a system that can ensure privacy. The reason for using cryptography for storing important information is to protect the confidentiality of information and also to improve productivity, integrity and to prevent unnecessary abuse.

The topic “design and implementation of a software used to send secured information” is an introduction of a security strategy to safeguard information stored and used by Nigerian Police. It is achieved by encrypting any confidential information put into it, using Encryption mechanism and then applying Decryption mechanism in order to extract the original information.

**PROBLEM STATEMENT**

The problem is security; the password method used in almost all commercial operating systems even those deployed in Nigerian Police, is probably not very strong against a sophisticated attacker. The choice of data Encryption comes next for the reduction of unauthorized access of confidential files.

**AIM AND OBJECTIVES**

The major objective of this study is to produce an Encryption software that will enhance data security in Nigerian Police

1. To highlight the features of information security
2. To ensure that maximum protection and authentication of information is achieved
3. To ensure that information access is to only authorized personnel of Nigerian Police
4. To highlight the dangers that may affect information
5. To help enhance information integrity
6. Implementation of a new Encryption Algorithm / Technique

**1.4 SIGNIFICANCE OF THE PROJECT**

Due to the importance of encryption, most organizations have devoted so much effort to device access control measures that will prevent unauthorized persons from getting access to information that does not concern them. The significance of this study is to ensure the confidentiality, accountability, integrity and availability of information security and privacy in Nigerian Police

**SCOPE OF THE STUDY AND LIMITATIONS**

The study is focused on designing an application using encryption and decryption techniques to safeguard the information stored in systems used by Nigerian Police in order to improve security and secrecy of company data.

Limitations encountered during this project study include :

* Poor power supply when developing software
* Lack of good text and journals on cryptography
* Inadequate finance
* Time constraint

**METHODOLOGY**

The existing system is manually carried out. Information on military signals is stored in an office file. Their personal data are being collected and each person has a file created for him or her. Search on these files takes time.

One has to go through the whole files in search of a particular record. This is cumbersome, hence the need for the computerization of the system.

**DEFINITION OF TERMS**

**ENCRYPTION**: This is the process of converting ordinary information into unreadable text/ cipher text.

**DECRYPTION**: This is the reverse of encryption, from cipher text to plain text.

**CIPHER**: Algorithm that handles the encryption and decryption process.

**CIPHER** **TEXT**: The unreadable text created after encryption.

**KEY**: Secret parameter that determines the functional output of the crypto algorithm or cipher.

**ALGORITHM**: A series of well-defined steps that can be followed to achieve a task or goal.

INFORMATION: A meaning full material derived from computer data by organizing it and interpreting it in a specified way.

SECURITY: This is the something that provides a sense of protection against loss, attack, or harm.

SYSTEM: Physical component of a computer that is used to perform certain task.

**PROJECT OUTLINE**

This is chaptered into five according to the related sections of the topic.

Chapter One contains the introductory parts of the study, definition, aims and objectives of the study, problem identification and the limitation of a software that is used to send secured information.

Chapter Two contains the literature review of the project work, the history of data encryption , also talks about previously designed computerized data encryption system.

Chapter Three contains the design process and analysis of the various components used in the construction of a computerized data encryption system.

Chapter Four contains the testing and maintenance procedure of the computerized data encryption system.

Chapter Five contains the summary of all that have been documented in the previous chapters the conclusions based on the findings of this project work and consequent recommendations extracted from the project work.

**CONCLUSIONS**

The importance of information security can never be underestimated , but the implementation of a computerized data encryption system ensures security at all times as it also protects them from sophisticated attackers, while its ability is to secure data information been sent. This project would go a very long way in providing security to banking information, academic information, sensitive database, hospital records etc.

**REFERENCES**

**Anderson, A.C. (2006).** Cryptography and network security. New York: A Bantam Press.

**Applied cryptography. (2001).** Computer security. U.S.A: CRC Press.

**Solomon, P.O. (November 2000).** Encrypting Messages. Russia: Encrypting Messages Centre.