DATA COMMUNICATION SECURITY ENCODED SYSTEM

(A CASE STUDY OF NATIONAL STEEL RAW MATERIALS EXPLORATION AGENCY, MALALI – KADUNA)

BY

MUSA, MOHAMMED MUSTAPHA

PGD/MCS/2005/2006/1192

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

SCHOOL OF SCIENCE AND SCIENCE EDUCATION

FEDERAL UNIVERSITY OF TECHNOLOGY

MINNA – NIGERIA

JULY, 2007

TITLE PAGE

DATA COMMUNICATION SECURITY ENCODED SYSTEM

(A CASE STUDY OF NATIONAL STEEL RAW MATERIALS EXPLORATION AGENCY, MALALI – KADUNA)

BY

MUSA, MOHAMMED MUSTAPHA

PGD/MCS/2005/2006/1192

THIS PROJECT IS SUBMITTED TO THE DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF POSTGRADUATE DIPLOMA IN COMPUTER SCIENCE

THE DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
SCHOOL OF SCIENCE AND SCIENCE EDUCATION
FEDERAL UNIVERSITY OF TECHNOLOGY
MINNA – NIGERIA

JULY, 2007

APPROVAL PAGE

This is to certify that this is an original work undertaken by MUSA, Mohammed Mustapha PGD/MCS/2005/2006/1192 and has been prepared in accordance with the regulations governing the preparation and presentation of project in Federal University of Technology, Minna.

....	30/08/2007. ....
Alh. D. Hakimi (Project Supervisor)	Date
....	....
Dr. N. I. Akinwande (Head of Department)	Date
....	....
External Supervisor	Date

DECLARATION

I hereby declared that this project has been conducted solely by me, under the close supervision and guidance of Alh. D. Hakimi of the Department of Mathematics and Computer Science, Federal University of Technology, Minna, Niger State and I have neither copied someone's work nor has someone done it for me.

Moreover, authors whose works have been referred to in this project have been duly acknowledge.

....	....
MUSA, Mohammed Mustapha	Date

DEDICATION

To my late father, May his soul rest in peace, “Ameen”.

ACKNOWLEDGEMENT

My profound gratitude to the Almighty Allah, The Bestower of Honour, for guiding and protecting me throughout the period of my stay in Federal University of Technology, Minna from inception of this program to date, and for seeing me through all my endeavours.

My special gratitude to Alhaji D. Hakimi (Sarkin Yakin Gini), my able supervisor, who guided me through this research work to date, without whom the authenticity of this project work is questionable, may Allah reward and bless you. I also express my gratitude to my Head of Department and to all the staff of the department both academic and non-academic staff for their usual cooperation and understanding, may Allah in His abundance mercy be with you all.

I am ever mindful of the love, courage, prayers and support of my lovely mother, my late father (May your soul rest in peace), my wife and children (Abdulfatah, Abduljaleel, Adamu and Nusaibah), I love you all so dearly. The entire staff of National Steel Raw Materials Exploration Agency, Malali, Kaduna, words cannot express how I feel about you all especially my mummy, Hajia Rabi'atu U. Sodangi, the Assistant Director Administration for her support, May Allah reward you, Ameen.

Nature will never forgive me, if I did not express my warmly appreciation to all my friends especially Bitrus A. Wovi of National Youth Service

Corps (NYSC), Minna who standby me in many aspect while undergoing this program, thank you Bitrus, may God make you to be successful in life. My friends in FUT – Minna and class mates, the experience is unforgettable one, thank you very much for your cares and support all these period, believe me I feel you all. Wish you all the best and God bless.

TABLE OF CONTENT

CHAPTER ONE: GENERAL INTRODUCTION

CHAPTER TWO: LITERATURE REVIEW

CHAPTER THREE: SYSTEM ANALYSIS AND DESIGN

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Data communication is concerned with the transmission (sending and receiving) of information between two or more locations. This proposed project " Data Communication Security Encoded System" will be solely concerned with the security of data transfer using encryption technology, that is, the confidentiality, authenticity, integrity and non-repudiation are basic concepts of security data delivery over an insure network. The proposed project will aim at, providing and ensuring data integrity and confidentiality, in order to achieve that security, cryptographic technology is introduced, where data can be encrypted in such a way that no unauthorized person can have access to it in a network that is not secure. However, it is recommended and advisable, unauthorized person are automatically ejected, because there is no way to decode, that is, decrypt the information without the right code, no right codes no information, period. We have examined cryptography, which is concerned with keeping communication or information private. Indeed the protection of sensitive information has been emphased throughout most of history.

CHAPTER ONE

GENERAL INTRODUCTION

1.1 INTRODUCTION

Communication in general is very important in our day-to-day activities, it is essential; it involves the ability, skills and proficiency to pass information across. The passing of information between two or more people helps in correcting or understanding a certain situation. Data communication involves the transfer of information or data from one medium to another or from the source to the destination.

Computer system on various networks can be connected together for effective transmitting of data from one location to another, its help to achieved some certain objectives, the said goal are achieved due to timely receiving of data and information, when the security encoded system is introduced the activities will be secured, because data security and confidentiality can be achieved successfully. Nevertheless any organisation using the security encoded system of data, that is, encryption technology, either on a local area network (LAN) or a wide area network (WAN) will benefit tremendously, the information or data are being converted into codes, whereby information privacy is guaranteed.

1.2 BACKGROUND OF THE STUDY

The Agency as one of the Federal Government Parastatal with a population of 540 staff has its headquarters located in Kaduna and eight (8) zonal offices located at Akure, Bauchi, Calabar, Gusau, Kaduna, Lokoja, Makurdi and Owerri. Thus, with those diverse offices, it will be more secure and easier to communicate data/information via communication channels e.g. radio message, telephone lines and the most effective and secure means, that is, the computer networking than to use the manual method of files movement which is usually prone to destruction and misplacement.

However, with the introduction of E-governance by the Federal Government, it will be mandatory for probably all the Federal Government Establishment to be connected to the internet in the near future for easy accessibility of receiving and sending of required data/information. The researcher in regard to this background is aimed at finding out how data and information will be protected by using security coded system or encryption technology.

1.3 BRIEF HISTORY OF THE CASE STUDY (NSRMEA)

National Steel Raw Materials Exploration Agency (NSRMEA), Kaduna is a Federal Government establishment (Extra Ministerial

Department). It is the Exploration Division of the defunct Nigerian Steel Development Authority [NSDA].

The Nigerian Steel Development Authority was established under Decree No. 19 of 1971 and was dissolved by Decree 60 of September, 1979 with which National Steel Council was established and later metamorphosing as the National Steel Raw Materials Exploration Agency (NSRMEA) in 1987. The Agency is formally established by Decree No 49 of 1992. It was set up to carry out exploration of natural raw materials for the production of iron and steel. Examples of minerals explored are iron-ore, limestone, cooking coal, dolomite, refractory clay just to mention few. The minerals are available at high quality of commercial and economical benefit to the nation.

However, the continuous exploration of steel raw materials that are naturally spread in different locations within the country brings about the setting up of diverse technical unit concerned with specific function which have necessitated the division of the Agency into five departments, which are as follows:-

1. Administration and Finance Department
2. Operations North Department
3. Operations South Department
4. Geological Services
5. Engineering Services

At present, the Agency is headed by Engr. Nkem Douglas Nsofor who is the Director/Chief Executive and assisted by Deputy Directors and Assistant Directors, whose head the various departments. Alhaji Aliyu Ibrahim is a Deputy Director heading the Administration and Finance Department; Mr. B. Adeyemo is Assistant Director in charge of Operations North Department, Mr. A. A. Fasasi Assistant Director Operations South Department; Engr. A. Salami is the Assistant Director Engineering Services and M. T. Oyinloye is the Assistant Director Geological Services.

1.4 STATEMENT OF THE PROBLEM

In an Agency that explores raw materials locally for steel industries with eight zones across the nation, it is not wrong to say that an effective communication between all levels of management, departments, and Zonal offices is very important since information is an effective communication and dissemination of information across the Agency.

However, it is not just the information that is communicated but also the security, privacy and the confidentiality of the information communicated that determines the extend of the value of the information in the Agency still remains the old conventional hand-to-hand delivery by office assistant. However, with the security encoded system the confidentiality of such information cannot be 100% guaranteed. Thus, this poses a serious treat to the confidentiality of the information that passes through all levels of the management.

Some of these problems cannot be over emphasised:

(i) Lack of effective communication protocols

(ii) Lack of information security

(iii) Less information delivery speed

(iv) Shortage of computer system and computer personnel.

1.5 AIMS AND OBJECTIVE OF THE STUDY

In a simple state the objectives of this study can be viewed as creating security system for the communication of information within the Agency.

However, the objectives of this research work are explicitly stated below.

(a) Provide and ensure a customized means of transferring data files from one computer to another within the Agency.

(b) To provides and ensure security of files being transferred within the Agency.

(c) To ensure reliability and integrity of information that passes from different levels of management

(d) To design software that will facilitate the encryption and decryption of information when transferred from one point to another

(e) To provide ease of access to information that is transferred between two or more computers in the Agency.

1.6 JUSTIFICATION OF THE STUDY

Ensuring the confidentiality of data can in general only be attained by the use of strong cryptographic procedures. This concerns naturally also the protections of secret, which are threatened by spying and hackers. In view of the important of the information as a factor for maintaining the competitiveness of our system, it is essential to meet this challenge.

Moreover, token should be impossible to forge and should be attached to one user to prevent their use when stolen. Biometric method tie a token to a user on a physical level (finger print), and password do so based knowledge. However, password without a token are insecure, after all, can crack any password that a person can remember.

1.7 SCOPE AND LIMITATION OF THE STUDY

In every research work, the area of study has to be clearly stated in other to form a basis for stipulated jurisdiction in which the project work will cover.

This research will only entails the security of data and information transferred across computers and networks which will specifically focused on the techniques of encryption and decryption of data through the use of encryption algorithm that will be implemented in the course of the research work.

The said research work will focus only on data and information transfer, form one point to another and the techniques of encryption and decryption of data and information, through the use of encryption algorithm.

1.8 HYPOTHESIS

The hypothesis stated below will be supported for or against the implementation of data/information communication security encoded system in the Agency via computer system.

1.8.1 Ho: Null Hypothesis

Views on the position of computer system as an integral part for a secure data/information communication network do not depend on the various levels (management, senior and junior) of staff in the Agency.

H_I: Alternative Hypothesis

Views on the position of computer system as an integral part for a secure data/information communication network depend on the various levels (management, senior and junior) of staff in the Agency.

1.9 DEFINITION OF OPERATIONAL TERMS

Definition 1.9.1

Communication Security: Bhatti (1995) define communication security as the protection resulting from all measures designed to deny unauthorised person information of value which might be desired from the possession and study of telecommunication.

Definition 1.9.2

Algorithm: D. Hakimi (2006) define Algorithm as a set of unambiguous rules that define how a problem or class of problems can be solved in a finite sequence of steps.

Definition 1.9.3

Protocol: is a set of rules and regulations that determine the meaning and format of frames, packets or messages exchange below peer entity.

Definition 1.9.4

Access: A specific type of interaction between a subject and an object that result in the flow of information from one point to the other.

Definition 1.9.5

Network Security: Bhatti (1995) stated that in communication security the protection of networks and their services from unauthorized modifications, destruction or disclosure is refers to as Network Security.

Definition 1.9.6

ADP system Security: Aronu, D (1999), stated that in computer security, all of the technologies safeguards and management procedures established and applied to computer hardware, software, and data in order to ensure the protection of organisational assets and individual privacy.

Definition 1.9.7

Local Area Network (LAN): Fapohunda, A (1995), define LAN as a system of hardware, software and a communications channel that connects devices in close proximity, such as a building housing an organisation such as FUT-Minna, Bosso Campus or National Steel Raw Materials Exploration Agency Headquarters.

Definition 1.9.8

Wide Area Network (WAN): Fapohunda, A (1995), define WAN as a system of hardware, software and communications channels that connects devices over a wide area of network via international agreement between national bodies.

Definition 1.9.9

Cryptographic Algorithm: David C (1998) stated that in data security, a set of rules specifying the procedure required to encipher and decipher data.

Definition 1.9.10

Cryptography: David C (1998), define Cryptography as the discipline, which embodies principles, means and method for the transformation of data in order to hide information content, prevent its undetected modifications or prevention of unauthorised user.

Definition 1.9.11

Encryption: David C (1998) stated that encryption is the coding of a clear text message by a transmitting unit so as to prevent unauthorized eaves-dropping along the transmission line; the receiving unit uses the same algorithm as the transmitting unit to decode the incoming message.

Definition 1.9.12

Decryption: Is the process of data decoded when the need arises.

Definition1.9.13

Password: A word or phase used to show that one is authorised to enter, pass a barrier.

CHAPTER TWO

2.1 LITERATURE REVIEW

There is need to review related literature that is known and tested, therefore literature review is an essential aspect of this research work, there are so many areas to be touched which in turn help the researcher to achieve the targeted or desired goal.

Data communication is an integral aspect of information technology and processing, thus the security of such information is an imperative aspect of data communication as it determine the integrity and validity of information that has been communicated.

On the other hand encryption technology is one of the fasted and widely used data security technique or measures that are in use today to protect data and information from unauthorised violation. This chapter deals with the review on data communication, data security, and detail study into encryption technology (cryptography technology).

2.2 BRIEF OVERVIEW OF DATA COMMUNICATION

Christopher E. (1993-2006) stated that Data communication involves the transmission of information from one place to another or the transmission of electronic data to and from remote transmission of electronic data to and from remote facilities, between workstation and even between computers. Thus, any type of information either analog or digital, are usually transmitted through telecommunication lines, satellite or coaxial cables.

Christopher E. (1993-2006) stated that computer represent data as digital signals, that is, using binary bits (1's and 0's) while telecommunication devices on the other land use analog signals, that are continuous physical qualities like transmitting of sound in various frequencies in wave patterns. Thus for data communication to be possible, these two separate technologies telecommunication and computing must marry.

In fact, data communications have become possible with the development of a hardware device called MODEM.

Badmus (2006), stated that the MODEM is an encoding/decoding device capable of transforming digital signal into a form suitable for transmission on telephone lines and vise versa. MODEM is an acronym that stands for modulation and Demodulation taken from the functions performed.

Badmus (2006) also stated that in order to establish communication links between two stations, it will be required that there should be a modem at each end (source and destination). A MODEM at the source will modulate digital signal into analog signal transmittable on the telecommunication line, while the MODEM at the destination will demodulate the analog signals back to its original digital form.

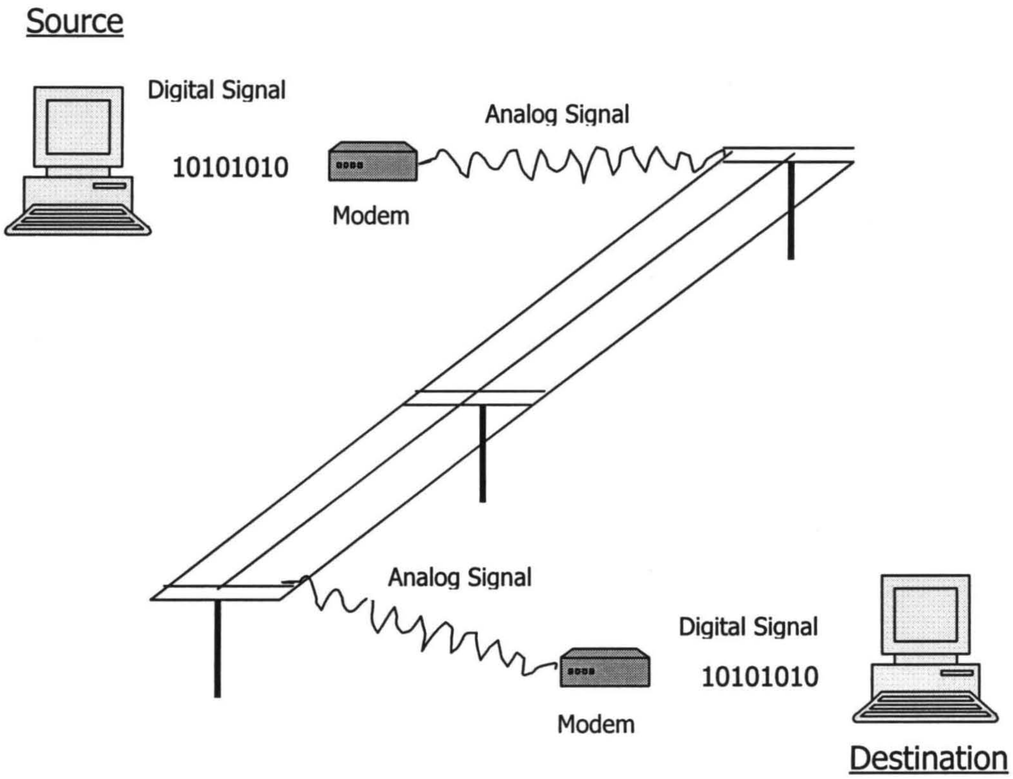


Figure 2.1: Communication Devices and Carrier

Source: Lecture note deliver by Prince A. Badmus on Introduction to Computer, PGD Maths and Computer, FUT-Minna (2006).

Badmus (2006); The wave signals exchanged by MODEMS are referred to as carrier signals. Carrier signals are modulated in three ways, by amplitude, by frequency or by phase. To represent digital patterns of zero and ones under amplitude modulation (AM), the magnitude, or voltage level, of the signal is charged. Higher amplitude can be used to mean 1 bit and lower amplitude 0 bit. With frequency modulation (FM), the frequency or number of oscillations of the signal per unit time, differentiated between the two binary digits. Phase modulation (PM) distinguishes bits by the location on the wave. Any of the three methods can be used for generating carrier signals to transmit digital information across communication channels.

2.2.1 Mode of Data Transmission

Bhatti S (1994) in his Lecture notes for M.Sc. Data Communication Networks and Distributed System D51 – Basic Communications and Networks classified communication channels on the basis of whether they are one-way, two-way but not simultaneous and simultaneous.

There are three transmission modes

1. Simpler
2. Half-Duplex
3. full-Duplex

Simplex: Bhatti (1994), A simplex link only carried data in a single direction. Example is (i) Test message in GSM (ii) Morse code sending.

Half-Duplex: Bhatti (1994), a half-duplex connection uses a single communication channel that alternates between sending and receiving modes. Half-duplex link allows data transmission in both directions to and fro but not simultaneously. The receiver of the message must want until the sender has completed transmission before using the channel. Examples (i) radio massage (ii) walkie-talkie.

Full-Duplex: Bhatti (1994), full duplex link carriers data in both ways to and from, and simultaneously too. In full duplex a two-way and simultaneously communications occurs between host computer and remote terminal Micro-computer. Example telephone conversation etc.

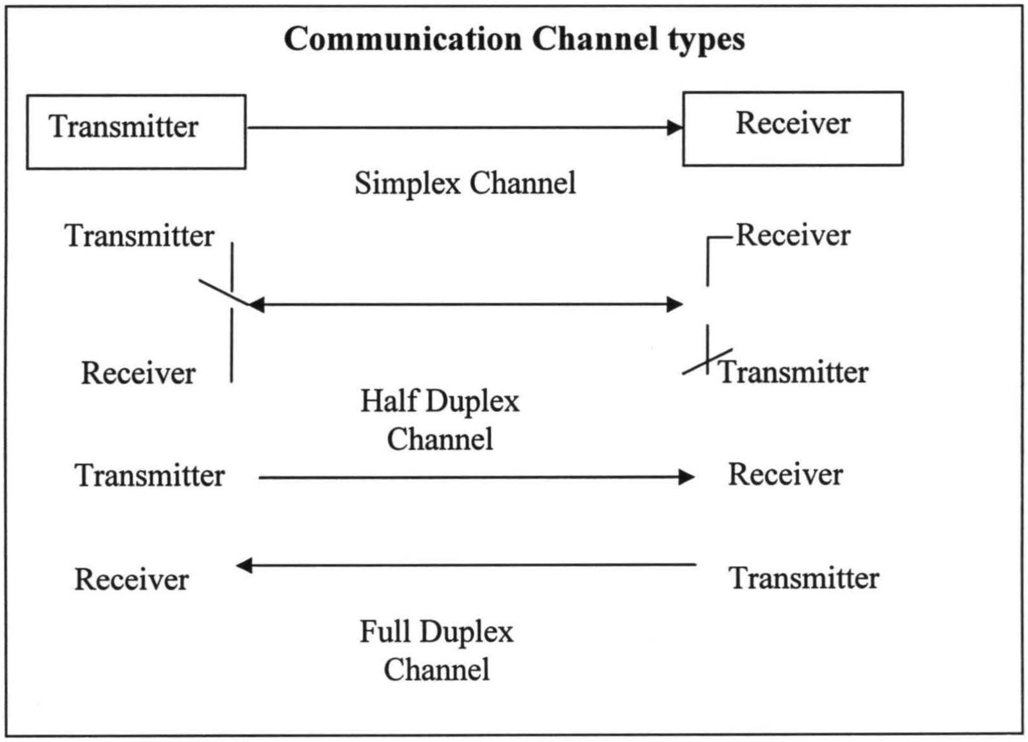


Figure 2.2: Communication channels source: www.comiresearch.com

2.2.2 Criteria for Data Communication Network

Bhatti S (1994) stated that the major criteria that a data communication network must meet are:

1. Performance
2. Consistency
3. Reliability
4. Recovery and
5. Security.

Performance: Bhatti S (1994), defines performance as the rate of transferring error free data. It is measured by the response time. Response time is the elapsed time between the end of an inquiry and the beginning of a response. Request a file transfer and start the file transfer factors that affect response time are:

(a) Number of users: more users on a network shows the network will run.

(b) Transmission speed: speed that data will be transmitted measured in bits per second (psb)

(c) Media type: type of physical connection used to connect modes together

(d) Hardware type: show computers such as XT or fast such as Pentiums

(e) Software type: how well is the network operating system (NOS) written.

Consistency: Bhatti S (1994) stated that, consistency is the predictability of response time and accuracy of data.

(a) User prefer to have consistent response times, they develop a feel for normal operating conditions, for example: If the "normal" response time is 3 second for printing to a network printer and a response time of over 30 seconds happens, we know that there is a problem in the system.

(b) Accuracy of data determines if the network is reliable! If a system has data, then the users will not have confidence in the information and will often not use the system.

Reliability: Bhatti S (1994), state that reliability is the measure of how often a network is useable. MTBF (Mean Time Between Failures) is a measure of the average time a component is expected to operate between failures normally provided by the manufactures. A network failure can be: hardware, data carrying medium and network operating system.

Recovery: Bhatti S (1994), defines recovery as the network's ability to ration to a prescribed level of operation after a network failure. This level is where the amount of lost data is nonexistent or at a minimum. Recovery is based on having backup files.

Security: Bhatti S (1994), stated that Security is the protection of hardware, software and data form unauthorised access. Restricted physical access to computers, password protection, limited user's privileges and data encryptions are common security methods. Anti-virus monitoring programs to defend against computer viruses are a security measure.

2.2.3 Data Communication Network Applications

Bhatti S (1994) lists the general applications of data communication network as follows:

(i) Electronic Mail (e-mail or Email) is the forwarding of electronic files to an electronic pool office for the recipient to pick up.

(ii) Scheduling programs allow people across the network to schedule appointments directly by calling up their fellow workers schedule and selecting a time.

(iii) Videotext is the capacity of having a 2 way transmission of picture and sound. Games like Doom, Hearts, distance education lectures etc.

(iv) Teleconferencing allows people in different regions to "attend" meeting using telephone lines

(v) Telecommuting allows employees to perform office work at home by "Remote Access" to the network.

(vi) Automated Banking machine allow banking transaction to be performed everywhere at grocery store, drive-in machines etc.

(vii) Information service Providers: provide connections to the internet and other information services. Example are CompuServe, Genie, prodigy, America on-line (AOL), etc.

2.2.4 Data Communication Errors

Bhatti S (1994). Human beings have developed intelligence, which makes them able to compensate for errors in transmitted data. It is feasible for a conversation to be held between two people even when only 30 percent of the data gets through intact. Computers are at the other end of the spectrum. One transmission error can spoil an entire dialogue. For this reason, error checking and prevention are basic requirement for all type of data communication.

Bhatti S (1994), stated that the protection against errors is usually affordable by adding extra bits to the packets that contain the data in a data pocket will be dedicated to error detection. The simplest means of using these bits is to set a parity bit a single digit that is set to make a sequence of bits add up to a value of 1 or 0. this is an effective way of finding single bit errors bit does nothing to help with two or any other even number of bits in error.

Bhatti S (1994), mentioned that more sophisticated technique known as check sums are usually employed. These are based on complex mathematics and are effective in finding many different errors types. Even more sophisticated are error correction technique. These tend to require a higher percentage of bits, but can actually correct transmission error hereby removing the need to retransmit entire packets for want of just one bit.

2.3 THE BASIC CONCEPT OF ENCRYPTION TECHNOLOGY

David (1988) stated that, encryption is refers to as the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from any one who might intercept it. Their effort to obtain the information will be fruitless unless they can crack the code that was used during the encryption process. Decryption is the reverse of encryption; it is the transformation of encrypted data back into understandable form.

David (1988) stated that encryption and decryption which stands for encoded and decoded data requires the use of a key. In modern cryptography, the key is a number that is plugged into an algorithm to produce the transmitted information. The length of the key determines how difficult it is to crack with every bit that is added to the key length, the amount of time and effort required to break the code increase exponentially for example is code took 3 days to break when the key is X number of bits ling, it will take a days to break if the key is (X-1) bits long and 27 days to break it if its (X-2) bit long and so on.

David C. (1988) stated that there are two types of cryptography algorithm that are normally used in conjunction with one another

(i) "private key" (symmetric cryptography)

(ii) "public key" (Asymmetric cryptography)

Before the rise of electronic commerce and the internet, private key encryption was acceptable so long as the data was not transferred. With private keys the key that is used to encrypt the data is the same one used to decrypt the data. Since the same key is used for both operations, private key is also referred to as "symmetric cryptograph".

When it became necessary for large amount of information to be sent across the world electronically, a problem arise since the key had to be transmitted along with it in same way, usually another means of communication was used, such the telephone, which makes the key just as vulnerable as the data would have been had it been sent unsecured. This problem was solved in

1976 when “Whitfield Duffie” and “Martin Hallman” developed public key cryptography. This type of encryption uses two keys that are different from one another but related in some ways. Since the two keys are different, public key is called “Asymmetric cryptograph”. One of the keys, the public key is distributed responsibly by the user to those who he will be sending information to the user also has a private key which he keeps to himself. The information is encrypted using the public key and transmitted along with the key. Then the receiver uses their private key to decrypt the data. Since the public key cannot be used to decrypt the information, there is no risk of the code being broken, so long as the private keys remain secure?

Another technological issue is the world of cryptography is that of “escrowed keys”.

2.3.1 Escrow Key

Encyclopaedia (2006). This type of cryptography provides certain third parties with the privileged of holding the keys to encrypted programs. These escrow agents would keep the keys secret unless ordered to release them by a court of law. Escrowed keys would allow law enforcement officials to read otherwise encoded information that could conceal criminal activity. While this type of cryptography provides strong encryption while giving the legal system an advantage in solving crimes, many feel that it is an unnecessary inversion of privacy by the government. This is a large area of policy debate where the interest of citizens in their own policy has to be balanced with the interest law enforcement officials.

2.3.2 Cryptography Protocols

David (1988) stated that as secured information became more and more important to the world organisations, are being more heavily relied upon to construct cryptography measures that offices higher levels of security. These measures are referred to as "protocols" and comprise an increasingly large portion of the product sold by large software companies like Microsoft.

David (1988), mentioned that another protocol is the Transport Layer Security (TLS), which has been proposed by the Internet Engineering Task Force (IETF) which is the body responsible for setting internet standard. All these protocols are simple public key encryption methods that only based on their speed, number of algorithms and number of bits per key.

2.3.3 Encryption Technology Overview

David (1988) stated that every encryption as stated earlier on is the process of observing data or information to make it unreadable without special knowledge. While encryption has been used to protect communication for centuries, only organisation and individuals with an extraordinary need for security have made used of it. In 1970s, strong encryption emerged from the sole preserve of secretive government, institution agencies into the public domains, and is now employed in protecting widely used systems, such as internet networks and secrets units.

David (1988) mentioned that encryption can be used to ensure secrecy, but other techniques are still needed to make communication secure, particularly to verify the integrity and authenticity of a message or information, for example, Message Authentication Code (MAC) or digital signature. Another consideration is protection against traffic analysis.

2.3.4 Ciphers

Bhatti S (1994) Stated that a cipher also spelt cipher is an (A precise rule specifying how to solve some problem) algorithm for performing (the activity of converting from plain text into code) encryption, a series of well define steps that can be followed as a procedure. On alternative term is encipherment the original information is known as “plain text” and the encrypted form as “cipher text”.

Bhatti S (1994); The cipher information contains all the information of the plain text, but is not in a format readable by human or computer without the proper mechanism to decrypt it, it should resemble Gibberish to those not intended to read it.

Bhatti S (1994); Ciphers are usually familiarised by a piece of auxiliary information key. The encryption procedures are valid depending on the key which changes the details operation of the algorithm. Without the key, cipher can not be used to encrypt or decrypt.

Ciphers versus Codes

Bhatti S (1994); In non-technical usage, a "(secret-computer science, the symbolic arrangement of data or instruction in a computer program or the set of such instruction) code" is the same thing as a cipher. Within technical discussion, however, they are distinguished into two concept codes work of the level of meaning i.e., words or phase are converted into something else. Ciphers, on the other hand, work at a lower level; the level of individual letters, small group of letters, or in modem schemes, individual bits. Some system used both codes and ciphers in one system, using "Super-cipherment" to increase the security.

Bhatti S (1994); Historically, cryptography was split into a dichotomy of codes and cipher, and coding had its own terminology, analogous to that for cipher; encoding, code text, decoding and so, however, codes have a variety of drawbacks, including susceptibility to (the science of analyzing and deciphering codes and cipher and cryptograms) Cryptanalysis and the difficulty of managing a cumbersome code book. Because of this, codes have fallen into disuse in modern cryptography, and ciphers are the dominant technique.

2.4 DATA ENCODED AND IMPLEMENTATION

Bhatti S (1994); Data security coded system is available as an off-the-shelf technology, and vendors after provide it as C code (sometimes as source code) areas a code for or already written. In either case, evaluating encryption implementations can be challenging, the algorithm may be strong, and the demo may run like a champ, but just how secure is the implementation? You can not easily tell by looking at the outside of a chip or at complex code. Attackers are ruthless and attempt to create faults in whatever ways they can. For example, attackers may not answer questions nicely, instead boundary a system with thousands of answers when the system requires only one and trying to blow a buffer (overflow) or can be boundary error that the system is unprepared to handle. Attackers search out vulnerability, such as areas in which sensitive information resides or how such information is shared. For example, poor pseudo random number generators unintentionally generate weak keys (invalid or "misinformed" data can cause errors in trusted code. You can after data limit and length and by passing all data through centralised validation checks versus checks scattered throughout the code).

Bhatti S (1994); Another importance difference among implementation is the packaging of the algorithm. A development kit for both hardware and software with a functional application programming interface, clear documentation, and code examples can be worth much more than you pay for them, in time to market savings. Many encryption companies offering engineering services, acknowledging that there is more to overall system security than the encryption algorithm itself. You can purchase various level of encryption from based data encryption to "complete" implementation, which include, digital signature, certificate-authentications management and support for smart cards.

Bhatti S (1994); Code and memory size (footprint) require a careful look. Many algorithms take the form of C source code-not assembly-for platform portability. When you evaluate an implementation, try to compile the code using several affect encryption speed, based on how it handles shifting operation. Also consider how efficiently the algorithm is coded. Because the bulk of encryption involves many hoops unrolling can significantly increase performance, allowing you to balance the specification of a high-performance processor and more memory.

Bhatti S (1994); If you need to interface to other systems and therefore other implementation of the same algorithm, proper implementation is important for preventing interpretability vulnerabilities. You can run your own validation tests, including the public tools manufacturers usually create when the industry adopts a standard. These tools pass test vectors through the implementation and compare the encrypted output with reference vectors. Additionally, remember that, although the algorithms themselves may be free, their implementations are not. Having to license three algorithms symmetric, asymmetric and high-increase costs, and you may have to license more than one of each to maintain legally compatibility. Finally be aware that export laws for encryption are complex and strict (see sidebar "exporting encryption technology").

2.5 DATA ENCODED TECHNIQUES AND PRECAUTION

David (1988): In data communication procedure, the receiver needs to know that the other party is indeed the right party and not a spotter. Verifying the identity of the sender is fairly straight forward. The sender encryption an identification (ID) message using he sender private key, and the receiver decrypts it using the senders public key. Communicators should use an ID message only once to prevent a spotter from using it later. A new problem arises, the public key must come from a trust worthily source. A hacker can access keys posted on a web page and replace the receiver's public key with the hackers own. This problem present in the middle attack in which a sender encrypts a message is using the attacker's public keys. The attackers intercepts and decrypts the message and then encrypts it using receivers public key and possesses the message on to the receiver the result is that neither party knows, that an attacker has intercepted or compromised the message. To answer this need, "certifying authorities" provide certificates containing public (now semiprivate) keys in a secure fashion using the certifying authority private key. But attackers can break certifying authority keys, forcing the certifying authority to revoke the certificates.

David (1988): Encryption involves a lot of cloak-and-dagger, and attackers can be complex and subtle. For every preventive measure, a corresponding counter measure exists. How careful your implementation needs to be depending on the calculated risk of data loss. In any case, keeping public keys relatively secret and frequently changing them should be an integral part of a system design, but don't count on the secretly to protect them. Attackers can compromise or gives secret code, if you don't employ a third party as a certifying authority; you take on the role yourselves and need to manage access of your own public keys.

2.6 APPLICATION OF ENCODED SYSTEM

David (1988): Despite all the precautions you can take to prevent the compromise of your encoded system, you should assume that some can and will break your encryption scheme. If an attacker discovers a back door, flow or vulnerability, you need to be able to recover and correct it.

David (1988): The first step is determined whether some one has breached your system. If the attacker's motive is to damage or crash your system, you will probably quickly find out. However, if the attacker wants information only to use it elsewhere, such as with credit card numbers, or to abuse a function such as adding value to a smart card, no fire work point this attacks. Filter can uncover this second kind of breach by observing the system behaviour and watching for aberration, such as a smart card account making an unusually number of transaction.

David (1988): Another method for detecting a breach is to keep a log of every transaction. In a set-top environment, only the home office should ever communicate with a code bar. Therefore, if the transaction log fails to match, then someone has attempted to contact the mode, signalling that someone may have compromised the mode. The more information you can capture, the better your chances of tracking down and understanding a breach. The problem arises, however, that an attacker can use any debugging hooks you include in the final product to compromise it, in order to be on the safe side.

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

3.1 SYSTEM ANALYSIS

System analysis is the practice of evaluating an erupting system to see how it works and how well it meets the user's needs.

This practice involved examining an already existing system for the new system to be introduced. The method is used with the primary aim of obtaining complete and adequate information, which will help in the development and design of a new system. The analysis helps in determining how best to use the computer with other resources to perform tasks, which meet the information needs of an organisation.

Several methods are involved in getting the analysis and other processes are involves in the investigation of the system to ascertain effectively how it works.

However, after a thorough feasibility study (that is a study to determine whether a plan is capable of being accomplished successfully: Sources: McGraw Hill Dictionary of Scientific and Technical Terms, Second Edition). There exist some problems and solution to the available existing system.

3.1.1 Problem of the Existing System

Non availability of staff records of the right/appropriate time for complete and accurate data updating. This problem can be surmounted if relevant information about staff records of employment and or resignation/termination of appointment can be communicated regularly to Computer Section.

The Computer Section is in need of more computer system, and modem software and the installation of network system within the headquarters and the Zonal offices. Similarly the Computer Section is in need of more computer professionals that can manage/handle and maintain the existing and new computers system.

Furthermore, the Computer Section is aimed at securing data and information of staff and other relevant information of the Agency, but this information is not fully secured, because files are not protected without the use of encryption technology i.e. password. Without an adequate security policy, the Agency is vulnerable to man threats including:

(i) theft of electronic and physical resources including data

(ii) Unauthorised modification of data

(iii) Fraud and other illegal activities

(iv) Disclosure of confidential and proprietary information

(v) Intentional errors earned by carelessness.

3.1.2 Solution to the Existing Problem

The main objectives of this project, is to design software that can be implemented to alleviate the problems associated with data security using encryption technology, which include the following:-

(i) No person or group of persons will be able to access, modify, add or delete the data illegally.

(ii) No unauthorised person or unauthorised group of person should be able to infer the value of confidential items, by manipulating queries or performing computations on released data.

(iii) The security arrangement will be flexible and the users provided with privilege, appropriate to their functions and needs.

(iv) Encryption and particularly decryption time will not materially affect the online needs operation. Encryption may in some system be performed on batches of data update, but encryption time will directly impact upon normal used access.

3.2 METHOD OF RESEARCH

Several methods were used in the investigation and also the gathering of information. The following method were used in the research work

(i) **Observation:** The existing manual system was studied and several faults were noted in it.

(ii) **Record Keeping-** The main purpose of this is to establish quantitative information, it was found out that the departmental objectives are not fully achieved and likewise the information needed for decision making is not readily available when it is required.

(iii) **Questionnaire:** this is a technique for getting answers to questions by using a form, which is filled by respondents, comparatively, in many ways questionnaire is similar to our interview, both interview and questionnaire attempts to get the feelings, benefits, experience or the activities of the respondents. They also may involve formats, which can be relatively structural depending on the situation.

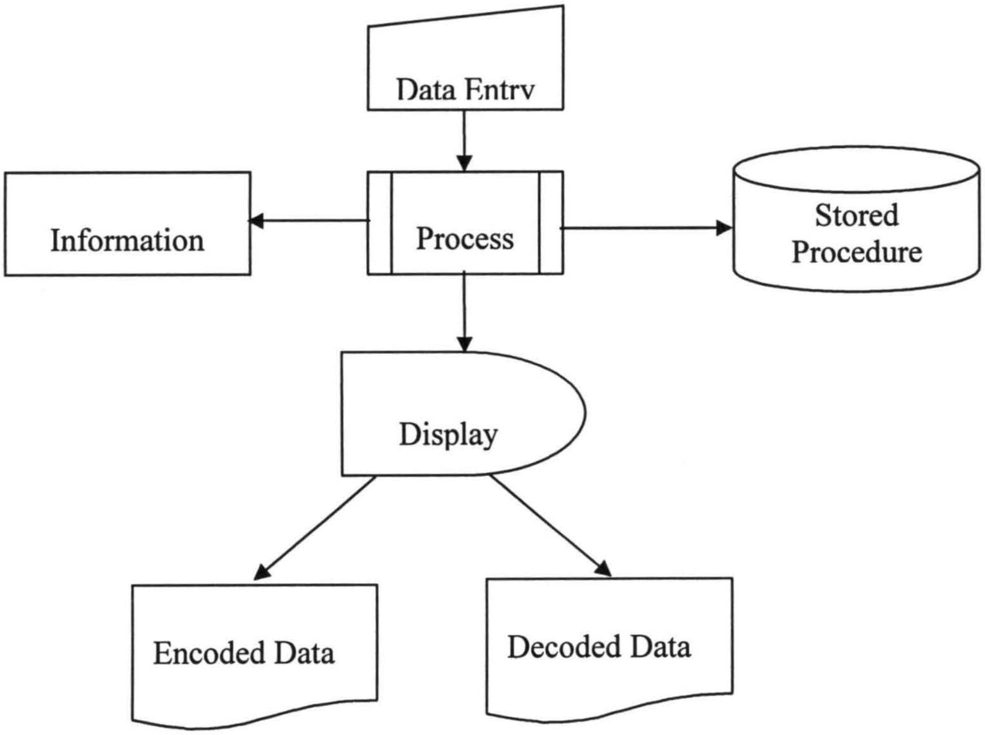
For this research work, the method of presentation was direct contact because of its advantages of less bias responses because of personal contact. The type of questionnaire used is the closed form (or structural) because of its simplicity and it is easy to administer and filled it, this is because it helps keep respondents mind fixed t the subject and facilitate the process of tabulation and analysis.

3.3 SYSTEM DESIGN AND SPECIFICATION

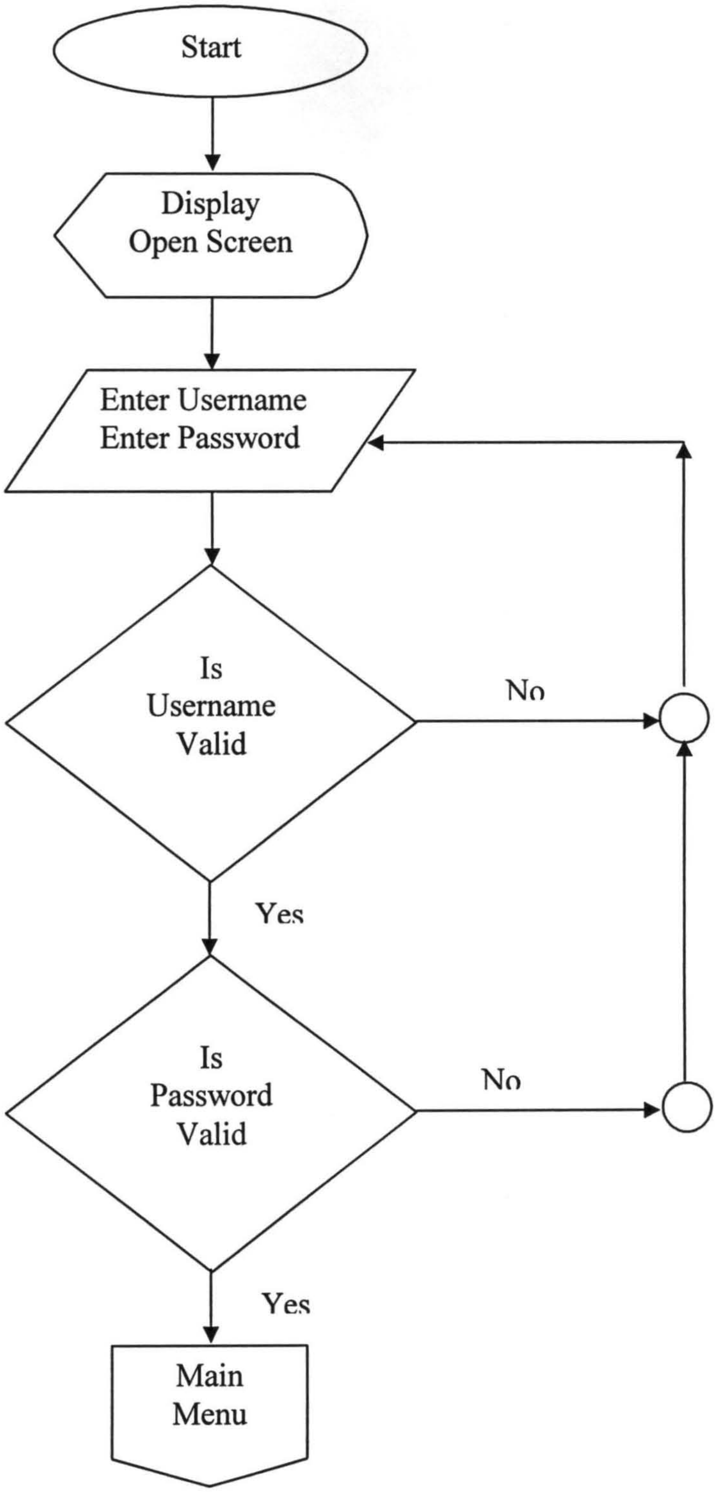
System design is the process of planting a new systems based on the findings of a system analyst. It is the use of creative ability and sense in organising logical bit, literally feasible procedure for a computerised system.

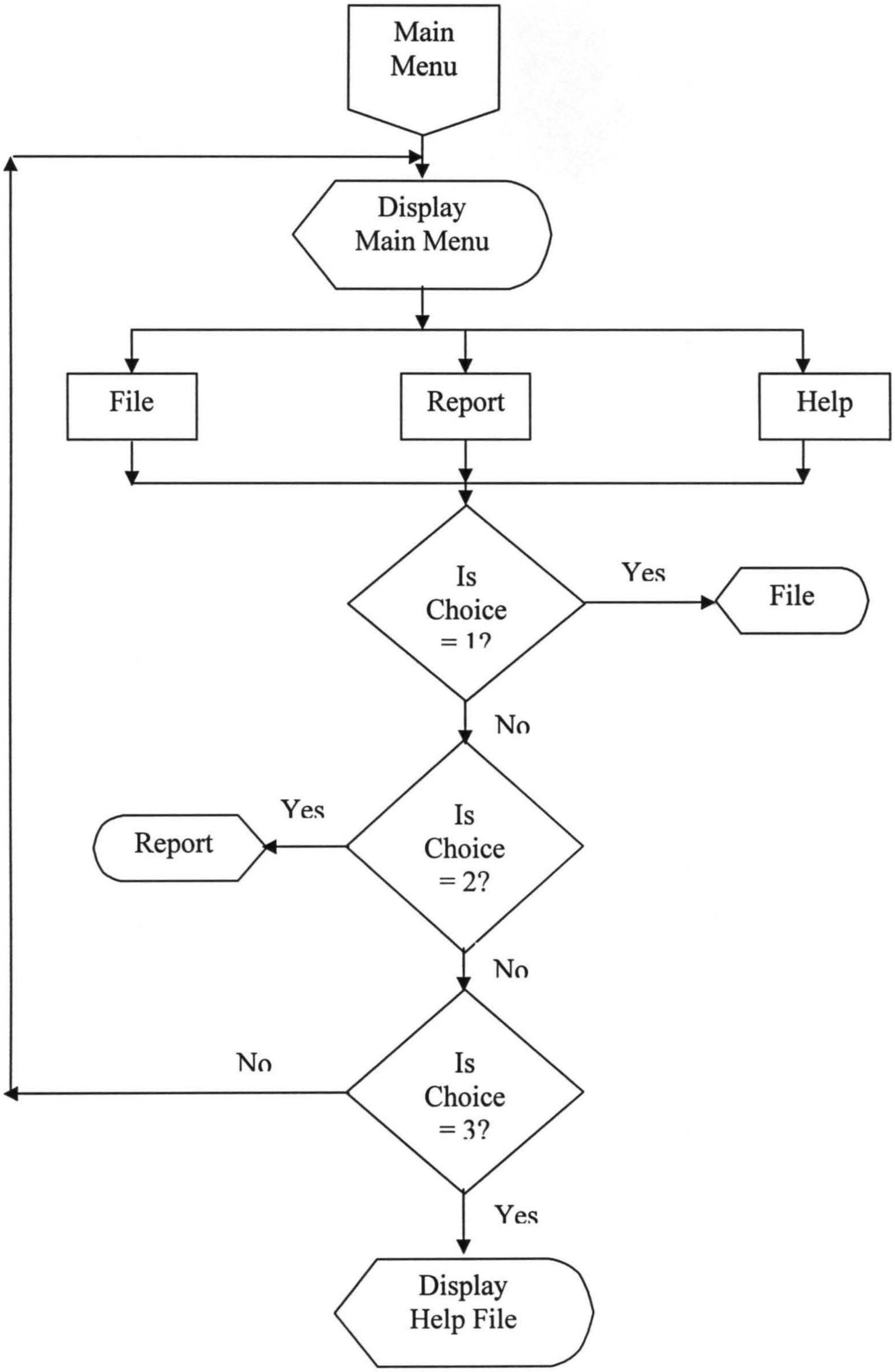
However, the general system design includes the flowchart (Procedure) a written explanation (Pseudo code) and database design or file design that contains data or information necessary to produce output. The database file design includes the entire database files used throughout the system for the proper storage of the activities general administration of the Agency.

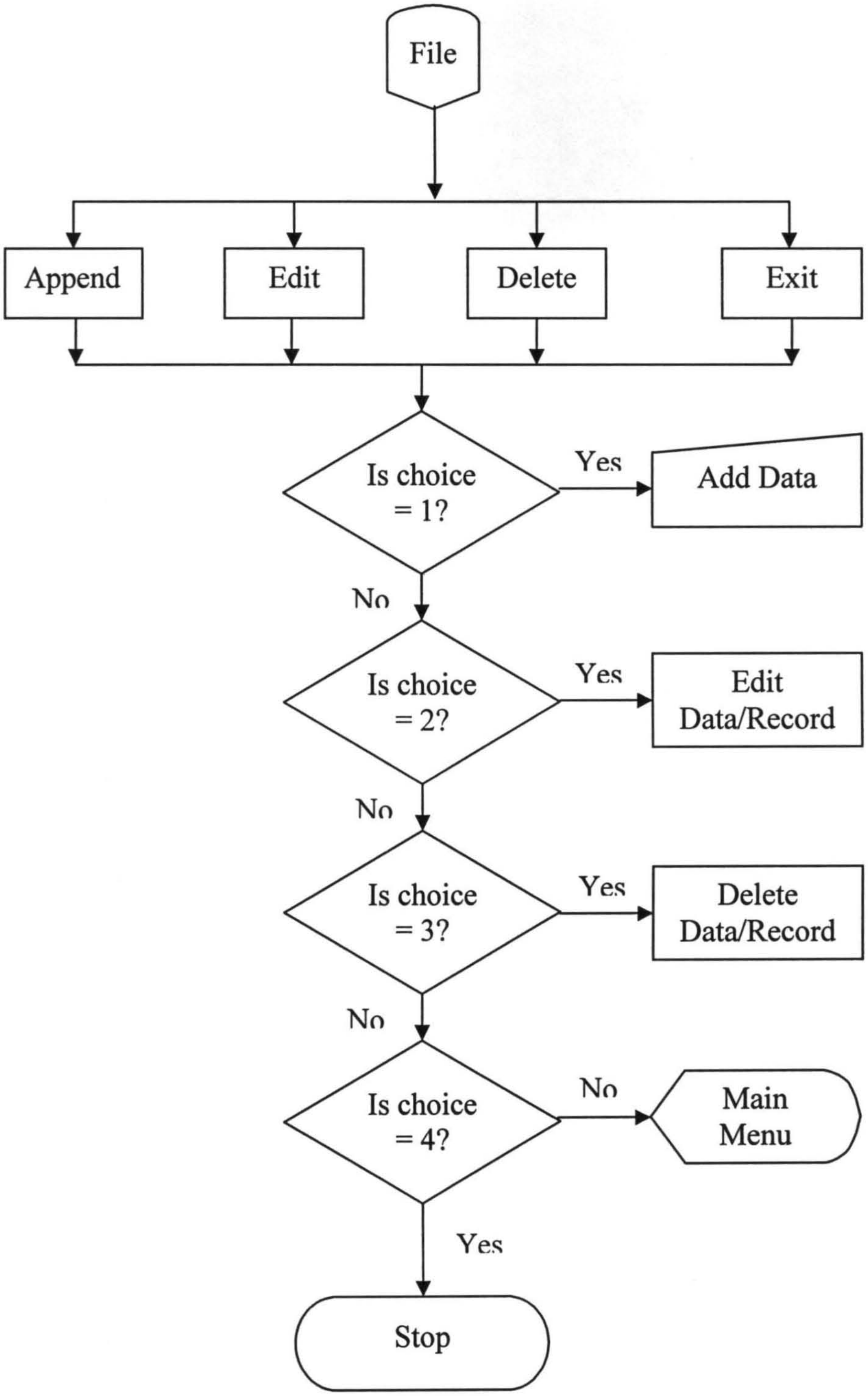
3.3.1 System Flowchart

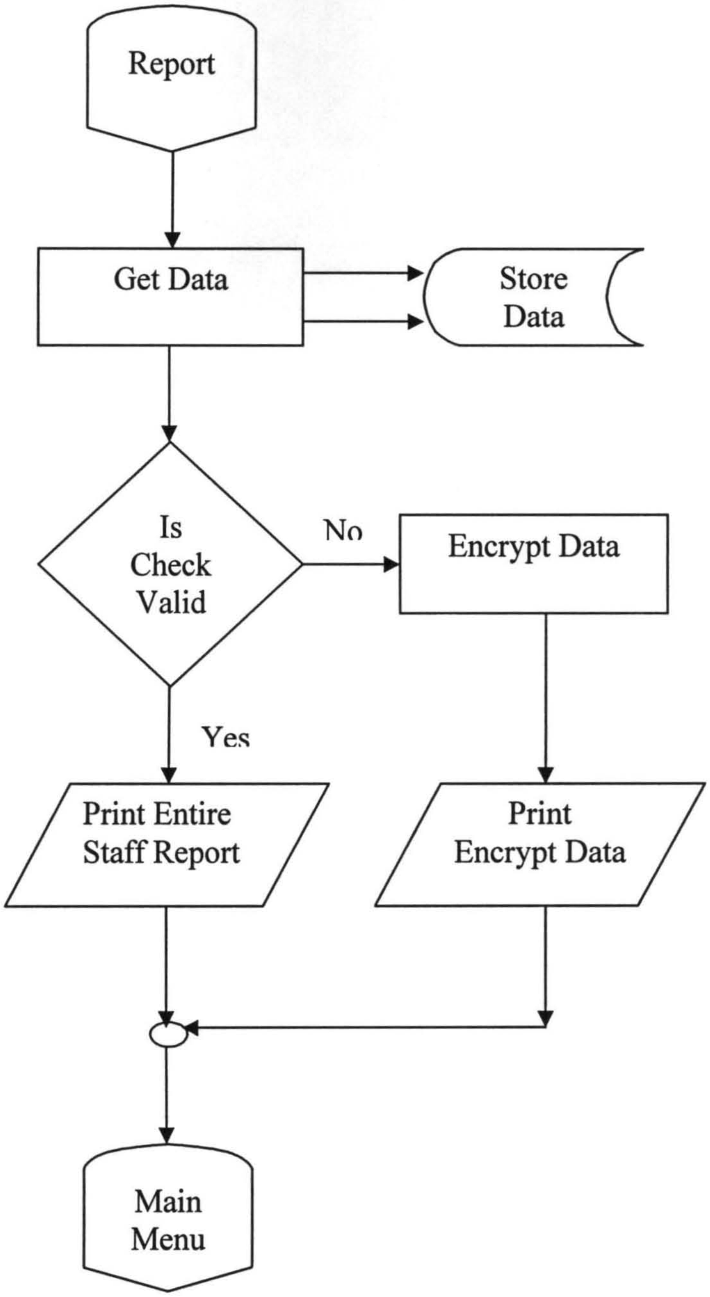


3.3.2 Program Flowchart




Main Menu
Display Main Menu
File
Report
Help
Is Choice = 1?
Yes
File
No
Is Choice = 2?
Yes
Report
No
Is Choice = 3?
No
Yes
Display Help File


File
Append
Edit
Delete
Exit
Is choice = 1?
Yes
Add Data
No
Is choice = 2?
Yes
Edit Data/Record
No
Is choice = 3?
Yes
Delete Data/Record
No
Is choice = 4?
No
Main Menu
Yes
Stop


Report
Get Data
Store Data
Is Check Valid
No
Encrypt Data
Yes
Print Entire Staff Report
Print Encrypt Data
Main Menu

3.3.3 System Requirement

These requirements for the effectual working of the system are the minimum hardware and software requirements for the development of the software to be design. Below are the minimum hardware and software for the development.

Hardware requirement

Below are the hardware devices that will be need for the system.

- ▶ A Pentium III 500MHZ or higher version.
- ▶ 15" Visual Display Unit Monitor (SVGA)
- ▶ Minimum RAM requirement should be 128MB or higher version.
- ▶ A Local Area Network (LAN) Installation.
- ▶ Hub
- ▶ UPS (Uninterrupted Power Supply)
- ▶ Surge Arrest.
- ▶ Printer
- ▶ Power Stabilizer

Software Requirement

- ▶ Minimum of Window 98 Operating System for remote and stand-alone computers, Window XP or higher version.
- ▶ Minimum of Windows NT Server Operating System for the Server (host) Computer.
- ▶ Visual Basic 6.0 Package.

3.4 CHOICE OF PROGRAMMING LANGUAGE

The language used for the coding of the software is Visual basic 6.0. This is a window-based object oriented programming language (OOP).

However, Visual Basic is the new and greatest incarnation of the old Basic Language. It gives a complete window application development system in one package. Visual Basic includes tools you can use to write codes in the simplest form and a complete help to help in debugging the errors.

Visual Basic itself is a window application you can code and execute applications with visual appearance like that of windows program. Today one needs a graphical tool that can work inside the windows system and create applications that takes advantages of all the graphical, multimedia, online and multi-processed activities that windows offer. It is such a tool, more than just a programming language. In fact, Visual Basic generates applications that interact with every aspect of today's windows operating system.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND PROGRAMME DEVELOPMENT

4.1 INTRODUCTION

This chapter presents the data collected, the analysis of which was based on the research questions. It also interprets primary data collected through the use of questionnaire.

4.2 DATA PRESENTATION, ANALYSIS AND INTERPRE TATION

The analysis is use to validate or nullify the earlier stated hypothesis based on the available sample data being collected. In doing this, statistical tool namely, the Chi-square (χ^2) is used (that is Test of goodness of fit).

A Chi-square test is computed as follows:

$$\chi^2 = \sum\left(\frac{O_i - E_i}{E_i}\right)$$

Where as Oi = Observed frequency

Ei = Expected frequency

A Statistical table is presented as Appendix II.

However, it will be based on this analysis that we can ascertain whether to continue with the research work and implement the new system or not.

4.2.1 Hypothesis Testing

Ho: Null Hypothesis H_I: Alternative Hypothesis

Ho: Views on the position of computer system as an integral part for a secure data/information communication network do not depend on the various levels (Management, Senior and Junior) of staff in the Agency.

H_I: Views on the position of computer system as an integral part for a secure data/information communication network depend on the various levels (Management, Senior and Junior) of staff in the Agency.

Relevant Information

Question four (4) of the questionnaire comprises of five (5) questions on Cryptographic Technology for some randomly selected staff in the Agency, ten (10) from each levels (management, senior and junior) of staff making a total of thirty (30) staff.

The responses from the respondents can be grouped as follows:

Strongly Agree Agree	Positive Responses
Undecided Disagree Strongly Disagree	Negative Responses

From the table 4.1 below, Q1, Q2, Q3, Q4 and Q5 represent question 1, question 2, ... and question 5 of the questionnaire, (see Appendix I). While the average represent the average on responses of questions and the group average represent averages for positive and negative responses.

Moreover, from the same table SA = Strongly Agree, A = Agree, U = Undecided, D = Disagree and SD = Strongly Disagree.

Table 4.1: Analysis of question asked on Cryptographic Technology "Data Security Encoded System". Case Study of NSRMEA, Kaduna

	Management					Senior					Junior					Total
	SA	A	U	D	SD	SA	A	U	D	SD	SA	A	U	D	SD	
Q1	6	2	2	0	0	6	3	1	0	0	4	3	1	1	1	30
Q2	7	3	0	0	0	7	2	1	0	0	6	3	1	0	0	30
Q3	8	2	0	0	0	6	3	1	0	0	5	2	1	1	1	30
Q4	7	1	1	1	0	5	3	2	0	0	4	2	2	1	1	30
Q5	6	2	2	0	0	6	2	1	1	0	4	2	1	2	1	30
Total	34	10	5	1	0	30	13	6	1	0	23	12	6	5	4	**150**
Average	6.80	2.00	1.00	0.20	0.00	6.00	2.60	1.20	0.20	0.00	4.60	2.40	1.20	1.00	0.80	
Group Average	**9**		**1**			**9**		**1**			**7**		**3**			

Table 4.2: Observed Frequencies (Oi)

Responses	Management	Senior	Junior	Total
Positive Responses	9	9	7	**25**
Negative Responses	1	1	3	**5**
Total	**10**	**10**	**10**	**30**

Calculation of Expected Frequencies

The expected frequency is calculated as follows:

$E_f = \frac{R_i \times C_j}{T}$: Where as:

E_f = Expected Frequency

R_i = Total for row (i)

C_j = Total for Column (j)

T = Grand Total

Substituting the above values:

$$E_{11} = \frac{25 \times 10}{30} = 8.33 \approx 8 \qquad E_{21} = \frac{5 \times 10}{30} = 1.66 \approx 2$$

$$E_{12} = \frac{25 \times 10}{30} = 8.33 \approx 8 \qquad E_{22} = \frac{5 \times 10}{30} = 1.66 \approx 2$$

$$E_{13} = \frac{25 \times 10}{30} = 8.33 \approx 8 \qquad E_{23} = \frac{5 \times 10}{30} = 1.66 \approx 2$$

Table 4.3: Expected Frequencies (E_i)

Responses	**Management**	**Senior**	**Junior**	**Total**
Positive Responses	8	8	8	**24**
Negative Responses	2	2	2	**6**
Total	**10**	**10**	**10**	**30**

For the computation of Chi-Square value, we use

$$\chi^2_{(r-1)(c-1)} = \sum \frac{(O_i - E_i)^2}{E_i}$$

Where as df = (r-i)(c-1) = degree of freedom

r = number of rows

c = number of column

α = 0.05

Table 4.4: Chi-Square Computation

Column/Row	Oi	Ei	$(O_i - E_i)$	$(O_i - E_i)^2$	$\frac{(O_i - E_i)^2}{E_i}$
1,1	9	8	1	1	0.125
1,2	9	8	1	1	0.125
1,3	9	8	1	1	0.125
2,1	1	2	-1	1	0.500
2,2	1	2	-1	1	0.500
2,3	3	2	1	1	0.500
		χ^2_c			**1.875**

Decision Rule: Accept Ho if $\chi_c^2 < \chi_t^2$

Reject Ho if $\chi_c^2 > \chi_t^2$

Decision:

$$\chi_c^2 = 1.875$$

$$\chi_{(r-1)(c-1)}^2 \; at \; \alpha = 0.05$$

$$\chi_{(2-1)(3-1)}^2 \; at \; \alpha = 0.05$$

$$\chi_2^2 \; at \; \alpha = 0.05 = (5.99)$$

Here χ_c^2 (1.875) < χ_t^2 (5.99), we therefore accept Ho. This implies that the position or view of a computer system as an integral part of modern data/information communication does not depend on the level of staff in the Agency.

However, based on the sample data, upon which the analysis is carried out, we can ascertain that computer is seen as a tool that can be use for a secure data/information communication network.

CHAPTER FIVE

DOCUMENTATION AND DISCUSSION OF RESULTS

5.1 INTRODUCTION

This chapter deals with the discussion of results, draw a conclusion and likewise give some recommendation for data communication security encoded system to the Agency.

5.2 DISCUSSION OF RESULTS

The researcher after an analysis of data obtained through the questionnaire administered to the various levels of staff and the new system developed comes up with the following findings:

- ► It was discovered and belief that the computer system is a vital tool for ensuring a secure means of data/information communication than the manual system of moving files containing data/information which is prone to destruction and misplacement between the various cadre/level of staff in the Agency.
- ► The new system developed based on the researcher's little knowledge is a data encoded system which has two modules:

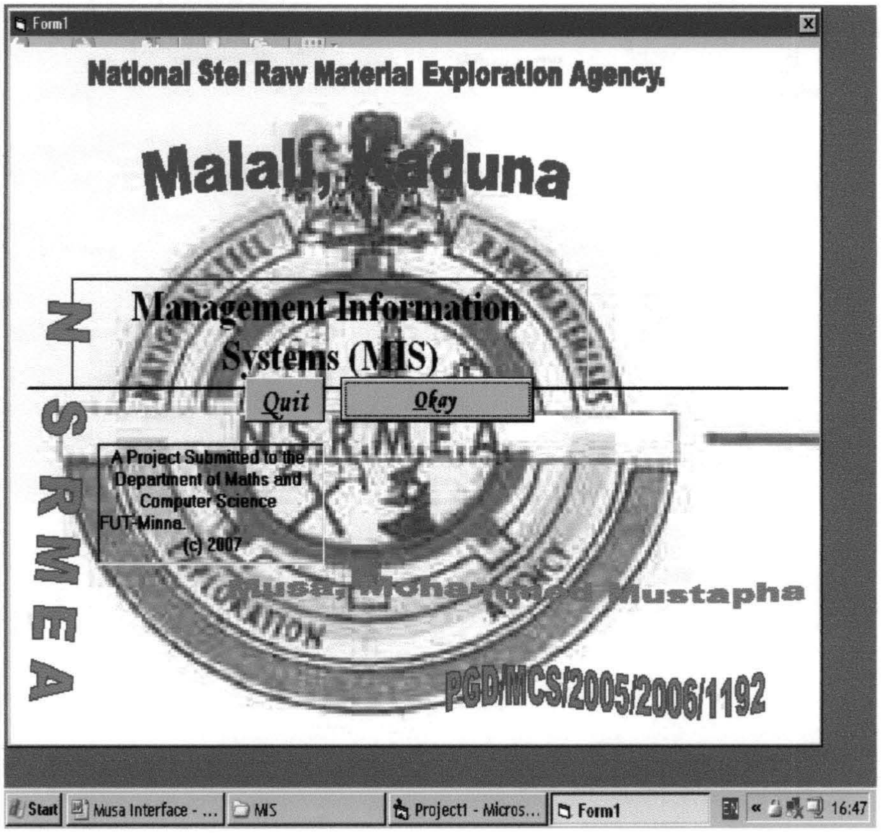
  (i) Data Enciphering (Encoded) Encryption

  (ii) Data Ciphering (Decoded) Decryption.

5.3 DOCUMENTATION AND ITS IMPORTANCE

5.3.1 Sample Output Forms

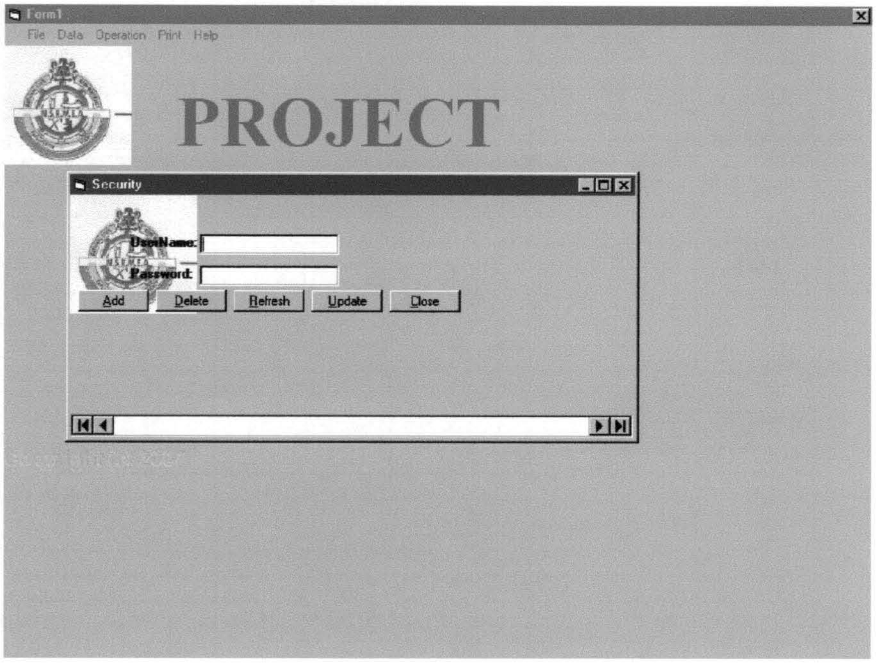
<u>Form 1</u>: Well come menu to Management Information System (MIS).


Form1
National Stel Raw Material Exploration Agency.
Malali, Kaduna
Management Information Systems (MIS)
N
S
R
M
E
A
Quit
Okay
N.S.R.M.E.A.
A Project Submitted to the Department of Maths and Computer Science FUT-Minna.
(c) 2007
Musa, Mohammed Mustapha
PGD/MCS/2005/2006/1192
Start
Musa Interface - ...
MIS
Project1 - Micros...
Form1
16:47

This is the well come menu or the main menu screen to the management Information System (MIS) of National Steel Raw Materials Exploration Agency (NSRMEA) Malali – Kaduna

Option Selection: This is the main menu that enables selection of either **quitting** the Management Information System (MIS) or **running** it by choosing okay.

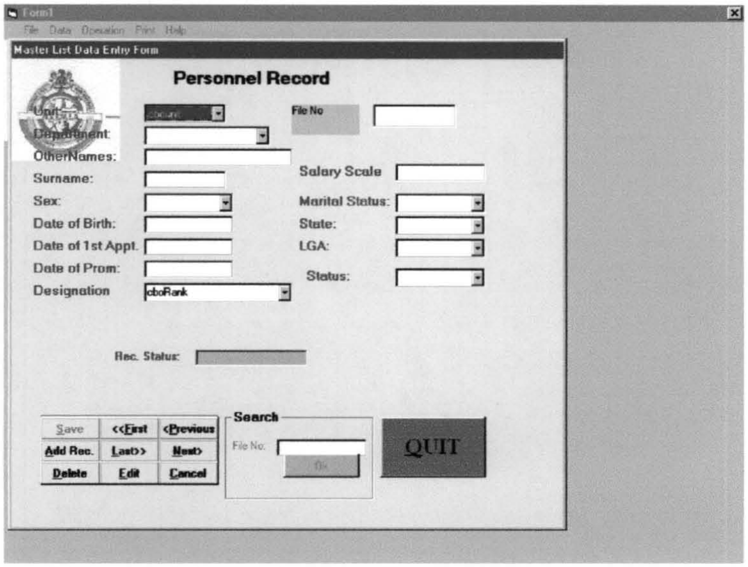
Form 2: Security Check Point



This is a display security menu being display after selecting okay from the well come menu.

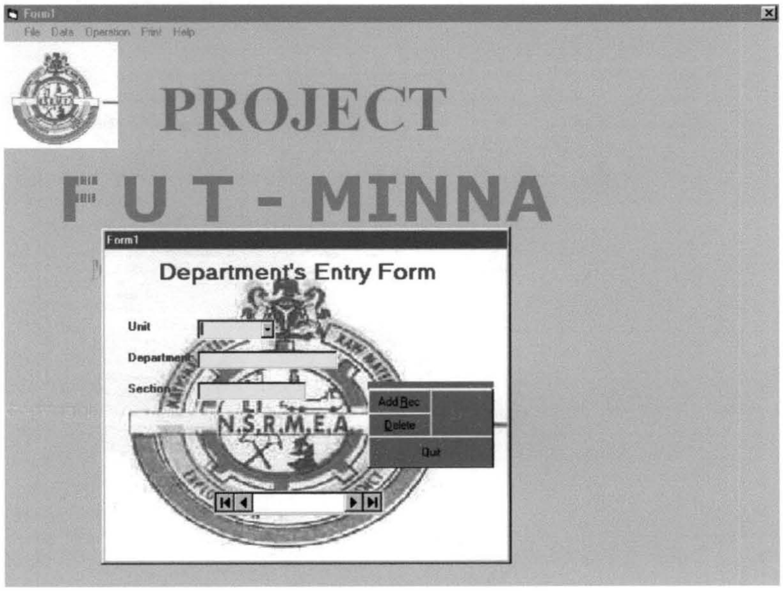
The user has to supply the appropriate username and password before he/she can be able to run the program.

Form 3: Personnel Record Data Entry and Editing Form



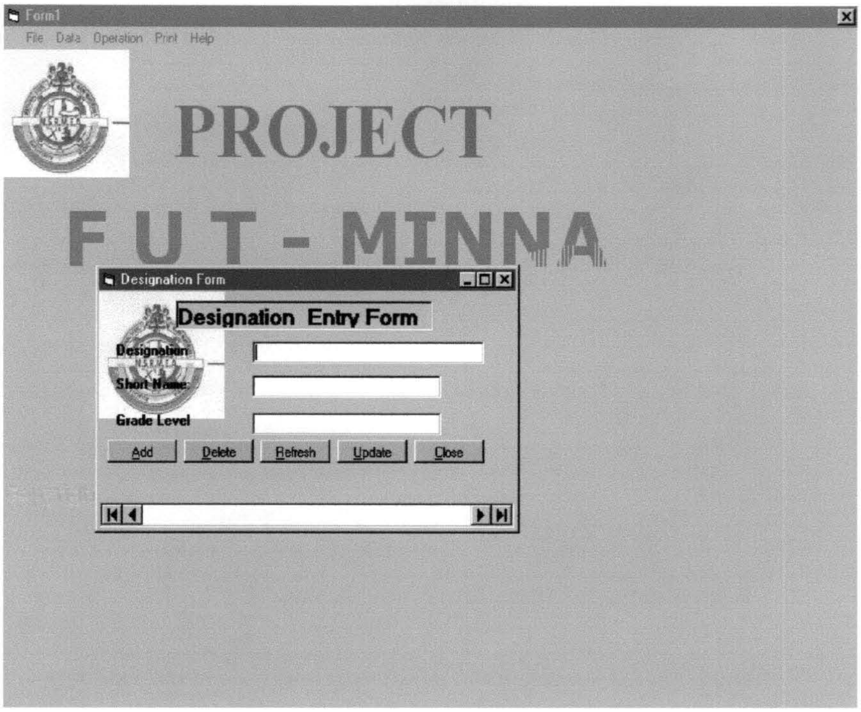
This menu is for data entry, editing for personnel record.

Form 4: Departmental Entry Form



This is use to enter an additional or edit department, unit or section.

Form 5: Designation Entry Form



This menu is use to edit personnel designation and grade level.

5.3.2 Input and Output Specification

Input Specification

The input is the data to be fed into the program by he programmer or operator during program execution either through the keyboard or other method of input.

Table 5.1: Input Specification data entry table

PRC:- 1239			
SURNAME	MUSA	DESIGNATION	PERSONNEL OFF.
FIRST NAME	MOHAMMED	DATE OF APPOINT.	99/99/9999
OTHER NAMES	MUSTAPHA	SS/LEVEL	10/09
DATE OF BIRTH	99/99/9999	DATE OF PROMOTION	99/99/9999
SEX	MALE	BASIC SALARY	120,000PA
MARITAL STATUS	MARRIED		
L.G.A.	HAWUL		
STATE OF ORIGIN	BORNO		

Output Specification

When the necessary data input is made, it will be processed and the information generated will be presented as either softcopy on the visual display unit (monitor) or as hard copy through the printer.

Table 5.2: Output Specification – Normal Report

NATIONAL STEEL RAW MATERIALS EXPLORATION AGENCY

(NATIONAL TEEL COUNCIL)

ENTIRE STAFF LIST AS AT 99/99/9999

SN	PRC No.	NAMES	D/BIRTH	STATE	LGA	DESIGNATION	D/1ST APPT.
1	1239	Musa, M.M.	26/10.1968	Borno	Hawul	Personnel Off.	01/02/1993
2	1249	Ajao, T.A.	10/05/1963	Osun	Ede/N	Asst. C Analyst	01/10.1993
3	1297	Abarta B.N.	20/02/1975	Gombe	Billiri	Secretary	29-10-1999

From the above staff listing of the output specification – Normal Report, it is possible to view and print the entire staff listing when needed.

Table 5.3: Output Specification – Abnormal Report

NATIONAL STEEL RAW MATERIALS EXPLORATION AGENCY

(NATIONAL TEEL COUNCIL)

ENCRYPTED: NON-AUTHORIZED USER

SN	PRC No.	NAMES	D/BIRTH	STATE	LGA	DESIGNATION	D/1ST APPT.
X	XXXX	XXXXXX	XXXXXX	XXXX	XXX	XXXXXXXX	XXXXX
X	XXXX	XXXXXX	XXXXXX	XXXX	XXX	XXXXXXXX	XXXXX
X	XXXX	XXXXXX	XXXXXX	XXXX	XXX	XXXXXXXX	XXXXX

From the table 5.3, the result of the staff listing can not be view neither printed as required by the unauthorized user.

5.4 CONCLUSION

In facts, encryption is about trust and preventing access to those without trust. Security offers the best result when employing a combination of counter measures.

However, encryption may seem trifle overdone. Cryptography tends to predict the worst to prevent surprises. Secure encryption, therefore, must balance protection, and assess performance, risk and cost in the pursuit of "sufficient security". One metric is that the more complicated your implementation, the more vulnerable it is aim for simplicity and the rest should follow.

5.4 RECOMMENDATION

Based on the findings carried out, we therefore recommend this system to the Agency for the following reasons:

(i) Ensuring data security in data files been transferred from one computer to another.

(ii) To provide access to information that is transferred between computer networks.

(iii) Ensuring safety of message between two communications.

(iv) Denying unauthorized users access to the system.

(v) To enable reliability and integrity of data and information across computer networks.

(vi) To ensure and provide a customised means of transferring data files from one computer to another within the Agency.

5.6 REFERENCES

(1) Arounu (1999) **Information System Technique with Internet Operations.** Volume 2. Ola Jamon Printers & Publisher, Nigeria

(2) Fapohunda (1995) **Understanding and Using Micro Computers**. AFLON Publishing Services Company, Abuja – Nigeria.

(3) Dennis & Williams (1995) **Information Security (Dictionary of Concept Standard and Terms)** Macmillan Publisher Limited, USA.

(4) David (1998) **The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability.** Online Documents.

(5) Christopher (1993-2006) **Data Communications Basics (A Brief Introduction to Digital Data Transfer)**. CAMI Research Inc., Acton, Massachusetts. www.camiresearch.com

(7) Bhatti (1994) **Lecture notes for M.Sc. Data Communication Networks and Distributed System D51 – Basic Communications and Networks**. Department of Computer Science, University College London www.cs.ucl.ac.uk/staff/S.Bhatti.

(8) Hakimi (2006) **Lecture notes for PGD Computer Science an Introduction to Algorithms**. Department of Maths & Computer Science, Federal University of Technology, Minna – Nigeria.

(9) Badmus (2006) **Lecture notes for PGD Computer Science an Introduction to Computer Science.** Department of Maths & Computer Science, Federal University of Technology, Minna – Nigeria.

(10) Goggle (2007) http://www.mste.uiuc.edu/patel/chisquare/kyprob.html

APPENDIX I

SAMPLE QUESTIONNAIRE

QUESTIONNAIRE

"Data Communication Security Encoded System" (A Case Study of National Steel Raw Materials Exploration Agency, Malali – Kaduna)

Instruction: Fill and tick ☑ √ the answer as appropriate against each question set below:

Name: ……………………………………………………………………

Department: ……………………………………………………………………

Status/Designation:……………………………………………………………………

Date: ……………………………………………………………………

1. Do you have any idea of what cryptographic technology is all about?
   Yes □ No □

2. How effective is the security of data transfer in the Agency?
   Very Effective □

   Effective □

   Fairly Effective □

   Not Effective □

3. Do you think the cryptographic technology will improve the security of data transfer from one point to another?
   Yes □ No □

4. It has been researched that cryptographic technology …………

(a) erase the problem of data interception by unauthorized person.

Strongly Agree □

Agree □

Undecided □

Disagree □

Strongly Disagree □

(b) is needed for encrypting security on vital information.

Strongly Agree □

Agree □

Undecided □

Disagree □

Strongly Disagree □

(c) ensure efficient computer oriented data communication to conventional mailing system.

Strongly Agree □

Agree □

Undecided □

Disagree □

Strongly Disagree □

(d) ensure and provide a customised means of transferring data files from one computer to another

Strongly Agree □

Agree □

Undecided □

Disagree □

Strongly Disagree □

(e) ensure reliability and integrity of information that passes from different levels of management, senior and junior staff.

Strongly Agree □

Agree □

Undecided □

Disagree □

Strongly Disagree □

APPENDIX II

STATISTICAL TABLE (CHI-SQUARE TABLE)

TABLE 26: PERCENTAGE POINT OF THE χ DISTRIBUTION

P	0.10	0.05	0.01	0.001
χ = 1	2.71	3.84	6.63	10.83
2	4.61	5.99	9.21	13.84
3	6.25	7.84	11.34	16.27
4	7.78	9.49	13.28	18.47
5	9.24	11.07	15.09	20.52
6	10.64	12.59	16.54	22.46
7	12.02	14.07	18.48	24.32
8	13.36	15.54	20.09	26.12
9	14.68	16.92	21.67	27.88
10	15.99	18.34	23.21	29.59
12	18.55	24.03	26.22	32.91
16	23.54	26.30	32.00	39.25
20	28.41	31.41	37.57	45.31
30	40.26	43.77	50.89	59.70
40	51.84	55.76	63.69	73.40
50	63.07	67.22	75.35	85.02

If χ is a random variable which has a χ^2 distribution with v degrees of freedom, the table gives the values which χ will exceed with the given probabilities.

APPENDIX III

PROGRAMME LISTING

```
Dim rs As Recordset
Dim rs1 As Recordset
Dim rs2 As Recordset
Dim rs3 As Recordset
Dim rs4 As Recordset
Dim rsR As Recordset
Dim rsD As Recordset
Dim rsS As Recordset
Dim rsL As Recordset
Dim db, db1 As Database

Private Sub cboState_Click()
   rsL.Filter = "State ='" & cboState & "'"
   Set rs4 = rsL.OpenRecordset
   cboLga.Clear
   With rs4
      .MoveLast
      .MoveFirst
      n = .RecordCount

      For i = 1 To n
         cboLga.AddItem (!Lga)
         .MoveNext
      Next i
   End With

End Sub

Private Sub CboUnit_Click()
   cboDep.Clear
   Call dept
   cboDep.Text = cboDep.List(0)


End Sub


Private Sub cmdDel_Click()
   On Error GoTo er2
   With rs
      .Delete
      .MovePrevious
      If .BOF Then
         .MoveFirst
      End If
      Set rs0 = rs.OpenRecordset
```

```
        Call assign
    End With
    Exit Sub
er2:
    MsgBox (Err.Description)
End Sub

Private Sub cmdEdit_Click()
    cmdsave.Enabled = True
    cmdEdit.Enabled = False
    ' Call assign

    With rs
        .Edit
        CboUnit.SetFocus
    End With
End Sub

Private Sub cmdfirst_Click()
    If cmdsave.Enabled = True Then
        cmdsave.Enabled = False
        cmdAdd.Enabled = True
        cmdEdit.Enabled = True
        cmdDel.Enabled = True

    End If
    With rs
        .MoveFirst
    End With
    Set rs0 = rs.OpenRecordset
    Call assign
End Sub

Private Sub cmdlast_Click()
    If cmdsave.Enabled = True Then
        cmdsave.Enabled = False
        cmdAdd.Enabled = True
        cmdEdit.Enabled = True
        cmdDel.Enabled = True
    End If
    With rs
        .MoveLast
    End With
    Set rs0 = rs.OpenRecordset
    Call assign
End Sub
```

```
Private Sub cmdnext_Click()
    If cmdsave.Enabled = True Then
        cmdsave.Enabled = False
        cmdAdd.Enabled = True
        cmdEdit.Enabled = True
        cmdDel.Enabled = True
    End If
    With rs

        .MoveNext
        If .EOF Then
            .MoveLast
        End If
    End With
    Set rs0 = rs.OpenRecordset
    Call assign
End Sub
Private Sub cmdprev_Click()
    If cmdsave.Enabled = True Then
        cmdsave.Enabled = False
        cmdAdd.Enabled = True
        cmdEdit.Enabled = True
        cmdDel.Enabled = True
    End If
    With rs

        .MovePrevious
        If .BOF Then
            .MoveFirst
        End If
    End With
    Set rs0 = rs.OpenRecordset
    Call assign
End Sub
Private Sub cmdOK_Click()
    On Error GoTo er1
    Dim ss As Boolean
    Dim n As Integer
    If txtfind.Text = " " Then
        msgok = MsgBox("No Search Record, Please", vbOKCancel)
        If msgok = vbOK Then
            txtfind.SetFocus
        Else
            txtfind.Enabled = False
            Label13.Enabled = False
            cmdok.Enabled = False
            CboUnit.SetFocus
        End If
    Else
        rs.FindFirst ("Fno ='" & txtFno & "'")
        'Set rs3 = rs.OpenRecordset

        'With rs3
            '.MoveLast
            With rs
            If .NoMatch = True Then
            'If .RecordCount = 0 Then
                MsgBox "Record Not Found, Please"
                txtfind.Enabled = False
                Label13.Enabled = False
                cmdok.Enabled = False
                CboUnit.SetFocus
            Else
                Call assign
'               cbounit = !unit
'               cboProg = !Prog
'               txtfrom = !dfrom
'               txtTo = !dto
'               txtNat = !nation
'               cboLevel = !Level
'               txtNo = !RegNo
'               txtSname = !sName
'               txtOnames = !Oname
'               cboRem = !Rem

                lblstat = "# " & Str(.AbsolutePosition + 1) & "/" & Str(.RecordCount)
                txtfind.Enabled = False
                Label13.Enabled = False
                cmdok.Enabled = False
                CboUnit.SetFocus
            End If
        End With
    End If
    Exit Sub
er1:
    MsgBox Err.Description
End Sub

Private Sub cmdAdd_Click()
    cmdsave.Enabled = True
    cmdAdd.Enabled = False
```

```
   cmdDel.Enabled = False
   cmdEdit.Enabled = False
   Call clea
   rs.AddNew


End Sub

Private Sub cmdSave_Click()
'   On Error GoTo er1
    Call assign2

    With rs

        .Update
    End With
    cmdsave.Enabled = False
    cmdAdd.Enabled = True
    cmdEdit.Enabled = True
    cmdDel.Enabled = True
    cmdAdd.SetFocus
    Exit Sub
er1:
    hd = MsgBox("EXISTING OR NULL File Number, Please", vbCritical, "Duplicate or
Wrong Number")
   ' rs.AddNew
    Call clea
End Sub

Private Sub Form_Load()
    On Error Resume Next  'GoTo er1
    cmdsave.Enabled = False
    Set db = OpenDatabase(App.Path & "/MIS")

    Set rs = db.OpenRecordset("Select * from Master order by Unit + Prog + Sname",
dbOpenDynaset)
    Set rsD = db.OpenRecordset("Select * from Department")
    Set rsR = db.OpenRecordset("Select * from RankTab")
    Set rsS = db.OpenRecordset("Select Distinct State from StateTab")
    Set rsL = db.OpenRecordset("Select * from StateTab Order by State")

    CboUnit.Text = CboUnit.List(0)
    'CboUnit.ItemData (1)
    With rs

        .MoveLast
        .MoveFirst
    End With
    With rsS
        .MoveLast
        .MoveFirst
        For k = 1 To .RecordCount
            cboState.AddItem (!State)
            .MoveNext
        Next k

    End With

    With rsR
        If .RecordCount > 0 Then
        .MoveLast
        .MoveFirst
        For k = 1 To .RecordCount
            cboRank.AddItem (!Rank)
            .MoveNext
        Next k
        End If
    End With

    Call dept
    Call assign
    Exit Sub
er1:
    MsgBox Err.Description
End Sub
Public Sub dept()
On Error Resume Next
    cboDep.Clear
    rsD.Filter = "Unit ='" & CboUnit & "'"
    Set rs3 = rsD.OpenRecordset
    With rs3
        .MoveLast
        .MoveFirst
        n = .RecordCount

        For i = 1 To n
            cboDep.AddItem (!dept)
            .MoveNext
        Next i
    End With
    Exit Sub
er1:
  MsgBox Err.Description
End Sub
Public Sub assign()
On Error Resume Next
  With rs
    CboUnit = !unit
    cboDep = !dept
    txtFno = !fno
    txtSname = !sName
    txtOName = !Oname
    txtDOB = !DOB
    cboMStat = !Mstat
    cboSex = !Sex
    txtNat = !nation
    cboState = !State
    cboLga = !Lga
    txtAppt = !ApptD
    txtProm = !PromD
    cboRank = !Rank
    cboStat = !stat
    txtHat = !Hat
    txtNOK = !Nok
    txtRelate = !Relate
    txtBasic = !Basic

    lblstat = "# " & Str(.AbsolutePosition + 1) & "/" & Str(.RecordCount)
  End With

End Sub
Public Sub assign2()
  With rs


    !unit = CboUnit
    !dept = cboDep
    !Prog = cboDep
    !fno = txtFno
    !sName = txtSname
    !Oname = txtOName
    !DOB = txtDOB
    !Mstat = cboMStat
    !Sex = cboSex
    !nation = txtNat
    !State = cboState
    !Lga = cboLga
    !ApptD = txtAppt
```

```
        !PromD = txtProm
        !Rank = cboRank
        !stat = cboStat
        !Hat = txtHat
    End With
End Sub
Public Sub clea()

        txtFno = ""
        txtSname = ""
        txtOName = ""
        txtDOB = ""
        'cboMStat = ""
        'cboSex = ""
        txtnation = ""
        'cboState = ""
        'cboLga = ""
        txtAppt = ""
        txtProm = ""
        'txtRank = ""
        'txtstat = ""
        txtHat = ""
        txtFno.SetFocus

End Sub
Private Sub cmdQuit_Click()
    frmMain.Enabled = True
    Unload Me
End Sub

Private Sub Frame2_Click()
    txtfind.Enabled = True
    cmdok.Enabled = True
    Label13.Enabled = True
    txtfind.SetFocus
End Sub




Private Sub cboUnit_KeyPress(KeyAscii As Integer)
    If KeyAscii = 13 Then
        KeyAscii = 0
```

```
      txtDep.SetFocus
   End If
End Sub


Private Sub txtdep_KeyPress(KeyAscii As Integer)
   If KeyAscii = 13 Then
      KeyAscii = 0
      txtLPrg.SetFocus
   End If
   Char = Chr(KeyAscii)
   KeyAscii = Asc(UCase(Char))
End Sub
Private Sub txtlprg_KeyPress(KeyAscii As Integer)
   If KeyAscii = 13 Then
      KeyAscii = 0
      txtSPrg.SetFocus
   End If
   Char = Chr(KeyAscii)
   KeyAscii = Asc(UCase(Char))
End Sub
Private Sub txtSPrg_KeyPress(KeyAscii As Integer)
   Char = Chr(KeyAscii)
   KeyAscii = Asc(UCase(Char))
End Sub


Private Sub cmdAdd_Click()
   cmdAdd.Enabled = False
   cmdsave.Enabled = True
   cbounit1 = CboUnit
   Data1.Recordset.AddNew
   CboUnit.Text = cbounit1 'CboUnit.List(3)
   txtDep = ""
   txtSPrg = ""
   txtDep.SetFocus
End Sub

Private Sub cmdDelete_Click()
   Data1.Recordset.Delete
   Data1.Recordset.MovePrevious
End Sub

Private Sub cmdQuit_Click()
   frmMain.Enabled = True
```

```
    Unload Me
End Sub

Private Sub cmdSave_Click()
    cmdAdd.Enabled = True
    cmdsave.Enabled = False
    Data1.Recordset.Update

End Sub


Private Sub Form_Load()
    cmdsave.Enabled = False
End Sub

Private Sub Data1_Reposition()
    With Data1

        .Caption = "Rec.#: " & Str(.Recordset.AbsolutePosition + 1) _
        & " of" & Str(.Recordset.RecordCount)
    End With
End Sub

ption Explicit
Dim txt As String
Dim db As Database
Dim rs As Recordset
Dim rs1 As Recordset
Dim rs2 As Recordset
Dim n, i As Integer
Dim prg, dt As String
Dim dt1 As Date
Private Sub Dat3_Click()
    frmMain.Enabled = False
    frmDepartment.Show
 End Sub

Private Sub Form_Load()

    dt = "05/05/2007"
    If dt >= Date Then
        End
    End If
End Sub

Private Sub mnRnk_Click()
```

```
  frmRank.Show
End Sub

Private Sub mnSec_Click()
  frmSecurity.Show
End Sub

Private Sub mnuexit_Click()
  Unload Me
  End
End Sub

Private Sub mnuitf_Click()
  frmhlpICTS.Show
End Sub
Private Sub mnumax_Click()
  frmMain.WindowState = 2
End Sub
Private Sub mnuMrec_Click()
  frmMain.Enabled = False
  frmMaster.Show
End Sub
Private Sub mnuOprNum_Click()
  frmprog.Show
End Sub
Private Sub mnuPrMlist_Click()
'   frmMain.Enabled = False
    prnNorm.Show

End Sub

Private Sub MnuPrPList_Click()
'   frmMain.Enabled = False
    prnEncrypt.Show
End Sub

Private Sub mnured_Click()
  Me.WindowState = 0
End Sub


Private Sub mnuState_Click()
  frmState.Show
End Sub
```

```
   frmRank.Show
End Sub

Private Sub mnSec_Click()
   frmSecurity.Show
End Sub

Private Sub mnuexit_Click()
   [illegible] Me

End Sub

Private Sub mnuitf_Click()
   frmhlpICTS.Show
End Sub
Private Sub mnumax_Click()
   frmMain.WindowState = 2
End Sub
Private Sub mnuMrec_Click()
   frmMain.Enabled = False
   frmMaster.Show
End Sub
Private Sub mnuOprNum_Click()
   frmprog.Show
End Sub
Private Sub mnuPrMlist_Click()
'   frmMain.Enabled = False
   prnNorm.Show

End Sub

Private Sub MnuPrPList_Click()
'   frmMain.Enabled = False
   prnEncrypt.Show
End Sub

Private Sub mnured_Click()
   Me.WindowState = 0
End Sub


Private Sub mnuState_Click()
   frmState.Show
End Sub
```

```
Private Sub mnuWriter_Click()
    frmhlpPrg.Show
End Sub

Private Sub st4_Click()

    Set db = OpenDatabase(App.Path & "/MIS")
    Set rs = db.OpenRecordset("Select * from MemoTab", dbOpenDynaset)
    With rs

        .MoveLast
        If .RecordCount < 2 Then
            frmMemo.Show
            Exit Sub
        End If
    End With

    frmLogin.Show
End Sub
```