TITLE PAGE

DATA SECURITY AND PRIVACY IN A STATISTICAL DATABANK

A COMPUTER APPROACH

(A Case Study of National Planning Commission)

By

JIMOH MUFUTAU IYANDA
PGD MCS/356/97

PROJECT SUBMITTED TO THE DEPARTMENT OF MATHEMATICS AND COMPUTER

SCHOOL OF SCIENCE AND SCIENCE EDUCATION
FEDERAL UNIVERSITY OF TECHNOLOGY MINNA, NIGERIA
IN PARTIAL FULFILLMENT OF AWARD OF POST GRADUATE IN COMPUTER SCIENCE

DECEMBER 1999

CERTIFICATION

I certify that this work was done by JIMOH MUFUTAU IYANDA under my supervision in the department of Mathematics and Computer. Faculty of Science and Science Education Federal University of Technology, Minna, Niger.

.....
Mr EZEAKO
(SUPERBVISOR)

.....
DATE

.....
DR REJU
(HEAD OF DEPARTMENT)

.....
DATE

.....
EXTERNAL EXAMINER

.....
DATE

ACKNOWLEDGEMENT

I am very grateful to almighty Allah for giving me the opportunity tom complete this laudable project. I am greatly indebted to my supervisor Mr Ezeako for his invaluable , meticulous and sincere supervision of this work.

My appreciation also goes to the other lecturers in University for their invaluable contribution to my knbowledge during the course of my programme. My special thanks goes to the other lecturers for their invaluable contribution to my knowledge during the course of the programme. My special thanks goes to Prince Badmus, Mr Raimi Kola, Dr Reju, Prof. Adeboye,others are Mr Adewale, Dr Yomi who have in one the other contributed to knowledge, I say thank you all.

My deepest appreciation goes to Alhaji Munir Ibrahim Lawal, Arc. Shakiru Suara, Rasheed Salman, Barrister Lawrence Adeosun, Raymond Osiberne, Bayo Mutiu, Charles Akonnor, Chuks Okoh for their love, moral and financial support through the course.

My special appreciation goes to friends on campus , frieds like Abdultalib,Olasunkanmi, Olajide Samaila Sodangi, Mrs Adem Ikwubiala, Hutman Toyin, and other who I can not mention and others who I can not mention but have weathered the storm with me., I say thank you for all your support.

TABLE OF CONTENTS

CHAPTER TWO

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

ABSTRACT

The study focussed on Data Security and Privacy in a Statistical Databank, a computer approach in National Planning Commission. The objective of the study was to examine the data security and privacy in the commission, and to examine the various lapses common to data security and privacy in the commission and to examine the various lapses common to data protection in a statistical data bank. In order to achieve this objective , various security measures were discussed to protect the vulnerability of data form illegal access by individuals who have no association with the organisation and if perpetrated ,how the tractor could be traced.

Meanwhile, emphasis were laid in Encryption as a form of security to protect the data, five major types of encryption were discussed.

It is however recommended that security measures should be taken seriously. This warning has become necessary because no matter how effective a security is, it becomes ineffective when the treat comes form within, that is why Artemiderous said to the Great Julius Ceasar in one of the Shakespeare plays that "Security gives Way to Conspiracy.

1.0 INTRODUCTION

Reliable data are responsible for policy formulation and development planning in every sector of any nation's economy. Clearly thought out and well formulated policies are necessary for setting development priorities and initiating new programs.

The issue of having a databank has gained prominence. Accurate data reflect true relationship with good planning. It must be noted that the national databank in general is weak, the paucity of reliable data has been responsible for the apparent lack of meaningful and sustainable planning in the country. The situation is compounded by the fact that most ministry do not keep appropriate records. Previous effort to address the situation has yielded limited result, as attempt by different ministry yielded different statistics. This has prompted the Federal Government of Nigeria to set-up NATIONAL PLANNING COMMISSION (MINISTRY) to co-ordinate and harmonize the various sector of the economy.

The National Planning Commission has put in place a workable arrangement for uniform data gathering and analysis which has enable the commission to properly monitor all sectors of the economy like industrial and business output, cost of production, employment ratio, external trade, internal debt, inventory balance of payment and its component, gross domestic product etc.

The commission has introduced a lot of security measure in order to maintain the security and privacy of the data stored. The National Planning Commission by taking this bold step would be following the steps taken by United States of America Government in

1977 when the government issued a report on violation of privacy relating to the computerized maintenance records. The two year focused on the enormous flow of personal medical purposes and the resulting invasion of privacy.

The reports concluded that safeguards must be applied to control both the access to any personal data and the type or data collected and stored.

The necessity for protecting data cannot be over emphasized. Data are exposed to many dangers in computing, such dangers includes: Un-authorized access, Virus attack, Manipulation of data for mischievous purposes etc. In this era, when the world has become a global village through international and internal networking computers now communicate with computers hundreds of kilometers apart, tactical information and even funds are transferred through advanced computer telecommunication networking. All these made computers highly vulnerable to mischievous attack through data manipulation which has made the issues of data security a great concern.

1.1 OBJECTIVES OF THE STUDY

The objectives of this research work includes:

(a) Definition of basic terms

(b) Detects the risks the computers are exposed in computing.

(c) Analyze existing measures against such risks

(d) Propose more effective measures where existing ones are found to be lacking.

1.2 SCOPE OF RESEARCH WORK

Data security is a wide area in computer science - However the research work is limited to the following :

- Encryption as a means of protecting data and information transferred in an Internet system from unauthorized access an eaves dropping.
- Problems and solution to computer virus
- How best to prevent and protect data in databank from un-authorized access.

1.3 DEFINITION OF BASIC TERMS

1.3.1 DATA:

This are fact that are certainly known from which valid conclusions can be drawn or made and it can also be information collected, prepared and operated or processed on a computer.

1.3.2 DATABANK

This can be regarded as a center whereby comprehensive information are stored and can be retrieved when required. It can also be defined as a center with a comprehensive file of computer.

1.3.3 DATA SECURITY

It involves the need to protect the corporate information database, its integrity and accessibility from unauthorized personnel.

1.3.4 CODE

Code can be regarded as a special mode of communication or encrypted which prevent eaves dropping or wire-tapping from an unauthorized individuals or organization.

1.3.5 PRIVACY

Privacy involves prohibiting an infringement or individual personal files, so that what is kept secret would be secret. Privacy also involves a situation whereby an individual or corporate organization is guarantee non-interference in their activities.

1.3.6 CONFIDENTIALITY

This is a situation in which the organization have developed confidence in their system and that the sensitivity of the information is assured. The sensitivity is such that information is sensitive if its unauthorized disclosure, modification (i.e. loss of integrity) or unavailability would harm the agency. In general , the more important a system is to the mission of the agency, the more sensitive it is.

1.3.7 ALGORITHM

An algorithm is a step-by-step of instruction for solving a specific problem. It can also be defined as a set of unambiguous rules that defines how a particular problem or class of problems can be solved in a finite sequence of steps.

Another way of defining algorithm is, as a list (i.e. a finite sequence) of instruction (each of which has a clear meaning) which can be carried out in a fixed order (with a finite amount of effort and time) to find the answer to a problem.

1.4 **SECURITY DESIGN PRINCIPLE**

1.4.1 ACCESS

This is a process whereby the user has a way to operate the system. That is the user gained access into the system by following all the required procedures on the system before any operation can be done.

1.4.2 USER ACCEPTABILITY

The security system must be acceptable to the user in order to put the system into maximum use. The human interface must be simple and easy to use and whereby it is not user friendly then the system would be rendered ineffective.

1.4.3 OPEN DESIGN SYSTEM

This is the process of exposing the design facilities to a number of people during planning stages which will facilitates correction before the system are implemented and also before the system can be rely on.

It is important to have open design in order to detects bugs earlier than in the long run when the designers of the security will not be available.

1.4.4 SEPARATION OF DUTIES

It refers to dividing roles and responsibilities so that a single individual can not subvert a critical process e.g. in financial systems, no single individual should normally be given authority to issue check. Rather, one person initiates a request for a payment and another authorized that same payment. In effect, checks and balances need to be designed into the process as well as the specific individual position of personnel who will implement the process ensuring that such duties are well defined is the responsibility of management.

1.4.5 LEAST PRIVILEGE

This refers to the security objective of granting users of only those accesses they need to perform their official duties. Data entry clerks, for example, may not have any need to run lysis reports of their data base. However, least privilege does mean that all will have

extremely little functional access; some employees will have significant access if it is required for their position. However, applying this principle may limit the damage resulting from accidents, errors or unauthorized use of system resources. It is important to make certain that the implementation of least privilege does interfere with the ability to have personnel substitute for each other without undue delay.

1.4.6 LEASE COMMON MECHANISM

Every shared mechanism represents a potential information path between the user. Therefore, this should be minimized, adhering to this principle would minimize the flows through operation on computer.

1.5 GENERAL PROTECTION MEASURE FOR STATISTICAL DATABANK

There are several protection measure existing which are used to protect data from unlawful accessibility from various individual or organization.

The statistical databank can make use of all the measure or used any one of them.

1.5.1 ACCESS CONTROL

This is done by assigning user access level that determine the user's file access and field access privileges. The file accesses privileges and field access privileges for a file are called its privilege scheme.

The user access levels are numbered 1 through 8. Assigning a low number gives the user greater access privileges. Assigning a higher number limits the user's access. However, only access level determines what the user can do with the file once it is accessed.

The access level securely can be worked at three levels

(I) User Access Level: This is the process whereby the user is those file and field access the user can access. The file and field given to a user is known as its Privilege Scheme.

(II) File Access Level: This is a privilege assigning to a user to determine the operations a user can do on the file. The access can be either to read, update, extend and delete. These privileges grant users the ability to

(i) View records in a file

(ii) Change records in a file

(iii) Append new records

(iv) Delete records from a file.

Field Access: At the field level, its possible to control what operations each user is allowed. You can grant full(FULL), read only (R/O) or no access (NONE) privilege to each field in a database.

1.5.2 LOG IN SECURITY

This may be used on a single micro-computer or in a local area network. The log in security allows to create a password protect system. If password protection is in force (1) No user can gain access to the system unless the user enters a valid log in. The log consist of three items: a group name, a log in name and a password.

1.5.3 DATA ENCRYPTION

Data encryption scrambles data, so that the scramble data can not be read until it is unscrambled. An encrypted file contains data that has been translated from source data to another form that make its contents unreadable. If the statistical databank is protected with encryption, the system automatically encrypt and decrypt files.

1.6 REASONS FOR DATA SECURITY IN A STATISTICAL DATABANK

Computers system security encompasses the security of all the information asset that constitutes the system be it manual or automatic. Security measures should not be taken just as the physical access and password. It should be noted that if hardware fails then the information system has failed. Therefore adequate measures should be taken regarding data stored in data bank.

It is pertinent to note that security in a statistical data bank prevent invasion of the corporate database, its integrity and accessibility by unlawful individuals or organization.

Also the security of statistical data bank gives assurance to the user that the information been used has not be tampered with, high level of confidence are then developed in the usage of the data.

1.7 VULNERABILITY OF A SECURITY SYSTEM

The vulnerability of any protected system be it data storage system or communication are numerous and most of them are discussed below.

1.7.1 TEMPORARY ASSIGNMENT AND IN-HOUSE TRANSFER

One significant aspect of managing a system involves keeping user access authorization up to date. Access authorization are typically changed under two types of circumstances

change in job role, either temporary e.g. (while covering for an employer on sick leave) or after in-house transfer and

Termination

User often are required to perform duties outside their normal scope during the absence of others. This require access authorization. However, additional authorization creates "Authorization creep" which have occurred with employees continuing to maintain

inconsistent with the principle of least privilege.

1.7.2 TERMINATION

Termination of a user's system access generally can be characterized as either friendly or unfriendly. Friendly termination may occur when an employee is voluntarily transferred, resign to accept a better position, or retires. Unfriendly termination may include situations when the user is being fired for caused "Rifed" or involuntarily transferred.

Fortunately both instances pose a security threat to the organization. For instance in a friendly termination is how confidentiality of data can be guaranteed? E.g. do employees know what information they are allowed to share with the public and in an unfriendly termination, the greatest threat from unfriendly termination is likely to come from those personnel who are capable of changing code or modifying the system or application. For example, system personnel are ideally positioned to wreak considerable havoc on system operators. This user can place logic bomb (e.g a hidden program to erase a disk) in code that will not even execute until after the employee's departure. There are even instances where code has been "held hostage" other employees can also cause damage.

1.7.3 CONTRACTOR ACCESS CONSIDERATION

Many Federal Agencies as well as private organization use contractor and consultants to assist with computer processing contractor are often used for shorter period of time than regular employers. This factor may change the cost of effectiveness of conducting screening.

The often higher turnover among contractor personnel generates additional cost for security program in terms of user administration.

1.7.4 PUBLIC ACCESS CONSIDERATIONS

system for electronic dissemination of information to the public. Some systems provide electronic interaction by allowing the public to send information to the government. (e.g. electronic fax filling) as well as to receive it. When system are made available for access by the public, additional security issues arise due to increased threat against public access system and the difficulty administrator.

Public access system are subject to a greater threat from hacker attacks on the confidentiality, availability, and integrity of information processed by a system.

Besides increased risk of hackers, public access system can be subject to insider malice. For example, an unscrupulous user, such as disgruntled employee, may try to introduce errors into data files intended for distribution in order to embarrass or discredit the organization. Attacks on public access system could have substantial impact on the organization's reputation and the level of public confidence due to the high visibility of public access systems.

Other security problems may arise from unintentional actions by untrained users. In public access system, users are often anonymous, this can complicate security administration.

CHAPTER 2

2.0 SECURITY MEASURES

Many important issues in computer security involve human users designers, implementors and manager. A broad range of security issues relate to how these individuals interact with computer and the access and authorities they need to do their jobs. No computer system can be secured without properly addressing these security issues.

Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position. Determining the appropriate levels is based upon such factors as the type and degree of harm (e.g. disclosure of private information, interruption of critical processing, computer fraud) individual can cause through misuse of the computer system as well. More traditional factors such as access to classified information and fiduciary responsibilities.

SECURITY ON PERSONNEL

The first step in staffing the computer center of the National Planning Commission is the process of screening and selecting. The process of screening and selecting helps determine whether a particular individual is suitable for a given position for example, the screening process help to ascertain the person's trust worthiness and appropriateness for a particular position. The screening process is formalized through a series background conducted through the personnel department.

After a candidate has been employed, the employees undergone training which includes which computer security responsibilities and duties.

Every member of staff of the computer center has a special identity card apart from the general identity card given to other member of staff. Also each member of staff has a special password allocated to them which are strictly confidential but only known to the

recorded finger of any individual that has any contacts with the system. There is also digital optical camera at the center which captures any image that entered the center.

USER ADMINISTRATION

Effective administration of users computer access is essential to maintain system security. User account management focuses on identification, authentication and access authorization. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations.

There is timely modifications or removal of access and associated issues for employees who are reassigned, promoted, or terminated or who retire.

USER ACCOUNT MANAGEMENT.

User account management involves

(1) The process of requesting, establishing, issuing, and closing user accounts.

(2) Tracking users and their respective access authorization and

(3) Managing these functions

User account management typically begins with a request from the user's supervisor to the system manager for a system account. If a user is to have access to a particular application, this request may be sent through the application manager to the system manager. This will ensure that the system office receives formal approval from the "Application Manger" for the employee to be given access. The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile.

System operators staff will normally then use the account request to create an account for the new user. The access level of the account will be consistent with those requested by the supervisor. This account will normally be assigned selected access authorization.

process. New user account are added and other are deleted. Permission change, sometimes permanently, sometimes temporarily. New applications are added, up graded and removed. Tracking this information to keep it up to date is not easy, but it is necessary to allow users access to only those functions necessary to accomplish their assigned responsibilities thereby helping to maintain the principle of *Least privileges.*

In managing these accounts, there is a need to balance timeliness of service and record keeping.

The managing of the user account is centralized in such a way that regional offices (states level) make a request in order to make necessary changes. The approval of these change is important, it may require the approval of the system or supervisor of the employee whose access is being changed.

AUDIT AND MANAGEMENT REVIEWS

From time to time, it is necessary to review user account management on a system. Within the area of user access itself, such reviews would examine the levels of access each individual has conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to=date, whether required training has been completed, and so forth.

Those reviews can be conducted on at least two levels

(1) On application -by- application basis or (2) On a system wide basis.

Both kinds of reviews can be conducted by, among other, in-house system personnel (a self-audit), the organization internal audit staff, or external auditors. For example, a good practice is for ***Application Manager*** to review all access levels of all application users every month and sign a formal access approval list which will provide a written record of approval. While it may initially appears that such reviews should be conducted by systems personnel, they usually are not fully effective. However because access requirement may change over time, it is important to involve application manager,

CATEGORY OF PERSONNEL THAT HAVE ACCESSED INTO THE COMPUTER SYSTEM

The various categories of personnel that have accessed into the computer system are discussed below

(i.) Head of Department:

The head of department acts as the administrative head of the center and is responsible for the co-ordinating and supervising the various activities in order to have a smooth running of the department.

(ii.) The Senior Officers

The Senior Officer from level 10 and above are allowed access into the computer system with the conditions that they are computer literate and they are subjected to proper monitoring in order not to cause damage to the system.(iii

The Analyst

This are responsible for modifying and refined the system to ensure that the system works efficiently, so that the objectives and goals of the commission are achieved.

(iii.) The Programmer

This is another set of people who are allowed access into the computer system, they are the blood stream of the system. They write the program used in the commission and also perform program documentation and rectify any problem which may arise from program documentation through programming.

(iv.) Data Entry Operator

This set of personnel are granted access into the system. The data entry operator enter data and programs into the computer but perform no verification. In fact, data entry operator has no right to change or correct any job submitted.

ACCESS TO HARDWARE AND SOFTWARE.

when proper complaints have been made about the malfunction of either the hardware or software.

The head of department would give approval for the correction or repairs to be made and any attempt made to repairs or correct any problem on the system is a criminal act and can lead to the terminating of the appointment of any staff involved.

SECURITY ON THE COMPUTER AGAINST ILLEGAL ACCESS

Security monitoring is an ongoing activity that works for vulnerabilities and security problems, and especially against illegal access.

Several security system are provided to monitor this problems, some of the measures are discussed below.

Check Summing Program.

This program presumes that files should not change between updates. They work by generating a mathematical value base on the contents of a particular file. When the integrity of the file is to be verified, the check sum is generated on the current file and compared with the previously generated value. If the two values are equal, the integrity of the file is verified.

Program check summing can detect viruses, trojan horses, accidental changes to files caused by hardware failures and other changes to files.

PASSWORD CRACKERS.

Check passwords against a dictionary (either a "regular" dictionary or a specialized one with easy-to-give passwords) and also checks if passwords are common permutations of the user.

INTEGRITY VERIFICATION PROGRAM

This can be used to look for evidence of data tampering, errors, and omissions.

and processing. These techniques can check data element, as input or as processed against expected values or ranges of values, analyze transactions for proper flow, sequencing, and authorization or examine data elements for expected relationships

These programs comprise a very important set of process because they can be used to convince people that, if they do what they should not do, accidentally or internationally, they will be caught. Many of these program rely upon logging of individual user activities.

VIRUS SCANNER

This are popular means of checking for virus infections. These programs test for the presence of viruses in executable program file.

INTRUSION DETECTORS

This analyze the system audit trail especially log-in, connectors, operating system calls and virus command parameters, for activity that could represent unauthorized activity.

System performance monitoring analyses system performance logs in real time to look for availability problems including active attacks (such as the 1988 Internet worm) and system and network slow down and crashes.

CHAPTER 3

3.0 SYSTEM DESIGN AND MODELING

This system was designed so as to give maximum protection for the data in a statistical data bank. There were lot of laxity found in the security measure of the organization studied. The inadequacies in the physical data security measures could be view as matters involving internal arrangement of the organization..

The organization could perform better if the following suggested solution are implemented. A software that automatically and permanently record the following is developed

(a) The identity of the operator that work in the organization's system.

(b) The nature of operation and the time, the operation was performed

(c) The file worked operated upon.

Such software could be developed and attached to all EXEC files so that it automatically spun to action each time such files are run.

The advantages of such " user monitoring device" include the culprit involved in data fraud to bed nabbed even long after such crime has been committed.

Employing log-in and simple enciphering techniques as presently done are not enough to guaranteed for security of data transferred through public lines. The major weakness includes: Not providing for log out mechanism after a number of unsuccessful attempt to log-in. It is mathematically provable that the probability of successful log-in will be directly related to number of trials i.e. let X denotes success in log-in to a system, and N to denote number of trial. We can say, an individual does not know the correct log-in number,

$$P(X) = F(N)$$

What the above simple equation implies is that the number of successfully log-in to a system increases with number of attempts. The Security implication is that a system become exposed to authorities access as the person trying to illegal log-in to the system line try different log-in numbers.

To guard against such risk, a provision is provided to log-out after a number of unsuccessful attempt for example, when any intruder, tried three different unsuccessful access codes, such intruder or non-intruder would be automatically log-out of the system network.

3.1 DESIGN OF A CRYPTOGRAPHY ON FILE SYSTEM

The nowadays use of computer controlled communication system, ask for special protection of data by crypto system, and cryptography provides efficient 'techniques of achieving this goal.' These crytographical techniques are methodologies for transforming the representation or appearance of message through communication representation or appearance of message through communication channel ensuring, its privacy and authencity, without changing its information content between the sender and the receiver.

The message to be transmitted or stored is called the plaintext. The process of transforming it and thereby locking the contents of the plaintext from being known to others (privacy) is called ***encryption*** or ***enciphering***. The transformed plaintext is called ***ciphered text*** or encrypted text or a cryptogram. The process of unlocking the ciphered text, to get back the original plaintext (message) is called decryption or deciphering.

Historically, the use of cryptography, which is the focus of this project, was exclusively confined to military and diplomatic communities, to guarantee the security of data being communicated. But in recent days, cryptography has gone public. Both private companies and corporate sectors alike have started using cryptography to protect the secrecy of

The importance of cryptography in teleprocessing cannot be over emphasized in time sharing environment, data can be physically protected since the most important data paths are centralized. In a geographical distributed network, like Natural Planning Commission, data vital to organization functioning are transmitted over communication links which physical protection are sometimes impossible and where possible uneconomical.

3.2 MODE OF IMPLEMENTATION

The program is implemented in pascal programming language. For this program, an interactive system is required, so there is a reliable and accessible system is advantageous. The program involves simulation of some enciphering and deciphering techniques.

The program starts off with an introduction of the author and then goes on to display the options available to the user. The options available are enciphering coded text, deciphering coded text and stopping option.

If the enciphering option is selected a list of the available enciphering technique are displayed in a menu like form. The message to be encipher must be resident on a diskette file. After selecting an enciphering technique, the user would be asked to indicate the location or name of the file. If an option that requires the use of a keyword (i.e. Vigener or 4 Runningkey) is selected, the keyword has to be supplied by the user.
Only an authorized user will be able to supply the correct keyword and hence decipher the code text.

After enciphering procedure has transformed text, the cipher text is stored in a file with the post fix "code". This coded forms is what can be transformed to the printer or transmitted in a network system. If the deciphering option is selected, the list of deciphering techniques is displayed which is the same as the list of enciphering techniques (but the procedure are in reverse order)
The cipher text to be deciphered must be resident **ON A DISKETTE FILE**. After

cipher text file. The appropriate keyword must be supplied on decoding the cipher text before it can be transformed or stored.

3.3 OPTIONS OF ENCIPHERING/DECIPHERING TECHNIQUE AVAILABLE

3.3.1 THE VIGENERE ROUTINE

For enciphering, the vigenere routine make use of a procedure which first convert each letter of the plaintext and the keyword to a numerical value and then this value is transformed using the formula

$$(I + J) \text{ Mod } 27$$

The value obtained is then converted back to a character. For deciphering, the same character conversion is carried out but it is transformed using the formula

$$(I - J) \text{ mod } 27$$

Where I is a character in the plaintext and J is a character in the keyword.

3.3.2 THE TRANSPOSE ROUTINE

For enciphering using the transpose routine, it breaks words of plaintext into blocks of five letters (including spaces) and then rearranges the letter according to the permutation

(1 2 3 4 5)

(2 5 1 4 3)

Meaning the first letter is substituted with the second, the second with the fifth, the third, fourth and third, fifth respectively. For deciphering, it is rearranged accordingly.

3.3.3 THE CAESAR ROUTINE

For enciphering, the Caesar routine uses the character conversion procedure and then transforms the value the formula is $(J + 3) \text{ Mod } 27$

The value obtained is converted back to character deciphering, character conversion is carried out using the formula.

$$(J - 3) \text{ mod } 27$$

3.3.4 THE RUNNING KEY ROUTINE

For enciphering and deciphering the transformation is similar to that of the vigenere method. The difference however is that whereas the alphabet can be shifted in the vigenere routine, it cannot be shifted in the running key routine. The formula for transformation (enciphering and deciphering) are basically the same.

3.3.5THE COLUMN ROUTINE, the Transformation is carried out by writing characters 000alternately on each two rows and then read row by row.

I AM A SURE WINNER

I M S R W N E

A A U E I N R

and is written as

IMSRWNE AAUENR

for deciphering, the ciphertext is reassembled accordingly.

CHAPTER 4

4.1 CHOICE OF THE PROGRAMMING LANGUAGE

Pascal is used as the programming language.It has a wide range of roles in areas of engineering ,scientific , statistical and mathematical application. It is generally a scientific language and is adaptable to suit many purposes of many people who may be interested in using the package.

4.2 HARDWARE REQUIREMENT

The program required the following hardware which would entrance its performance and this includes

a. Pentium
b. 16MB RAM
c. 2.1 GB Hard Disk
d. 1.44MB (3.5') Floppy Disk
e. CD ROM (x 23)
f. 14" SVGA Monitor
g. Enhanced Keybaord
h. YGA Adaptor
i. Laser Jet Printer
j. U.P.S (500 Volts)
k. Serial Mouse

4.3 COST AND BENEFIT ANALYSIS

Initially , the cost of designing a new system especially when it comes to the security look very high in a short run but when compared with the long run effect the benefit outweigh the cost.

Procurement of the system hardware system and the software development was 1.5m which was believed to be very high initially but compared to the security benefits in the long run , it is realised to be cost effective

For example with this system , it is difficult for an intruder to log in and access any information in the system. And again there is a high level of employee satisfaction because of confidence they have in the system.

4.4 # PROGRAM

USING PASCAL HIGH LEVEL LANGUAGE.

```
WriteIn    (”   1.   Vigenere    “)
WriteIn    (”   2.   Transpose   “)
WriteIn    (”                    “)
WriteIn    (”   3    Caesar      “)
WriteIn    (”   4    Running Key “)
WriteIn    (”                    “)
WriteIn    ( ”  5    Columnar    “)
WriteIn    (”                    “)
WriteIn    (”   6    Exit        “)
WriteIn    (”   ???             “)
WriteIn    (”   Select from options using number on the left of option
                desired”)
End:
Procedure  Chr  (var Letter: xter: Number: Integer);
Begin
Letter:= Copy ( “A B C D E F G H I J K L M N O P Q R S T U V W X Y Z”); Number;
If Number : = 0 then letter: = “  ”;
End.
Procedure ord (Var Number: integer; Letter; xter);
Begin:
 Number; pos (letter , “ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z);
End
Procedure Encipher; ( * The Enciphering Procedure *)
```

```
Procedure vigenere; (* To encipher using the vigenere's algorithm *)
Begin
For K: = 1 to length (sentence) Do
Begin
ord ( I , character {K J ) ;
ord (J , key { K J);
J:= (I + J) mod 27
chr   (K I, J);
Newsence: = concat (Newsence, C(KJ);
End;
End;
Procedure Transpose: (* To encipher using the transposition method*)
Begin
        I: - 1;
While I <=length (sentence) Do
Begin
L: = (length (sentence)  - I ) mod 5 );
If <>o then for J:= 1 to L Do
Word: = Concat (word, "  ");
Word:= copy (sentence , I, 5);
Transpose: = Concat (copy (word, 2, I), copy (word, 5,I) copy word 1, I ) copy  (word 4, I )
Transpose:= Concat (Transp., copy (word, 3, 1);
Newsence:= Concat (Newsence, transp.);
I;: = 1 + 5;
End;
End;
Begin;
```

```
Begin
ord. (J, character {I};
J:= (J + 3) mod 27;
Chr (c {I}, J);
Newsence:= Concat {Newsence, C ( I) };
Number := Pos (letter, "ABCDEFGHIJKLMNOPQRSTUVWXYZ);
END
Procedure:  Caesar (* To Encipher using the Caesar's algorithm)
Begin
For I:= 1 to length (sentence) Do
Begin
ord (J, character (I);
        J:= ( J + 3) mod 27
chr © (I ), J );
Newsence:= concat (Newsence, c (I);]
Begin
End;
End;
Procedure Runkey: ( * To Encipher using the Running key cipher*)
Begin
For K:= 1 to length (sentence) Do
ord. (J, character {K J};
ord. (I, key (KJ);
J: = ( I + J) mod 27


chr (c ( k), J;
```

```
End;
End;
Procedure Columnar ( * To encipher using the columnar transposition *)
                    (* Using the backwards method of encipherment and the Raul)
Begin
For I:= Length (sentence_) down to I Do
J:= length (sentence) -I + 1;
c (J) := character (I)
 End ;
K:= I
L:= Round (Length (sentence )/2 ):
for1:= J to L Do
 Begin
J:= 2 * I -1);
c(K):= character (J);
K:= K + I;
End;
Begin (main menu)
Repeat
Menu;
Read (option);
If (option = 1') or (option = "4") then
Begin


WriteIn        ('Input cipher key');
ReadIn(key stream);
```

```
key (I_):= copy (keystream, I, 1);
End;
WriteIn        (Device "input text");
While not E Of (f) Do
Begin
ReadIn(f. sentence): Newsence:= ' '
character {I}:= copy (sentence, I,1);
WriteIn        (Device, sentence);
If option:=    '1' then vigenere else
          :=   '2' then transpose else
          :=   '3' then Caesar else
          :=   '4' then Runkey else
          :=   '5' then columnar:
WriteIn        (Device);
WriteIn        ("Since this is supposed to be a secrecy");
WriteIn        (System not all the codes generated on the screen");
WriteIn        (Device);
WriteIn        ("Press space bar to continue);
ReadIn
WriteIn        ("Due to the nature in the system stores')
Write in       ("Files by storing anything that is entered to");
Write in       ("The system as, text, to Decipher");


WriteIn        ("you first key in the text to be deciphered");
WriteIn        ("Then save it, after which you go to the filler');
WriteIn        (" Mode and use the change option to change the text to code");
```

```
WriteIn      (Device);
Procedure Menu
Begin
Page (input);
WriteIn
WriteIn      (" Do you wish to encipher encoded text")
WriteIn      (:"Decipher coded text");
WriteIn      (" Transfer text');
WriteIn
WriteIn      (" stop program");
WriteIn
WriteIn      ???
WriteIn      (" select from option using character or left of bracket of option desired");
End;
Procedure prefer;
Begin
End;
Begin        (* main program*)]
              Welcome
WriteIn      (" Input preferred output device in full);
ReadIn
Rewrite      (Device, P: rename);
Read
Repeat
Begin
Readied      (Decision);
page         (Out put)
```

```
Begin
WriteIn      (" Encipher...");
WriteIn      (" indicate name or location of file to be enciphered")'
ReadIn (filename);
If (filename = "console') or (filename = 'I" ) then
Begin
Reset (f, filename);
Rewrite  (G, ' Bad I: Pow, code");
End          (* if console option is wanted *)
Else
Begin
Reset (f, concat, (filename, 'text);
Encipher
close (G, lock);
Rewrite end, concat (filename "code');
Else
Begin, if decision = D' then
Begin
WriteIn      ("decipher...");
WriteIn      (" indicate name or location of file to be deciphered')
ReadIn (Filename_);
Reset        (F, concat (filename 'code');
Rewrite       (G, concat "text");
Decipher
Close        (S * Lock);
Reset        (S * concat (filename, 'text);
End
```

```
Begin
WriteIn      ("Transfer...");
WriteIn      (Transfer which file (Please indicate where text or code )?;
ReadIn       (Filename)
Rewrite      (G, filename);
Transfer;
End;
WriteIn      ("output...");
WriteIn
Screen:=     O
While not E of (G) Do
Begin
Screen:=     Screen + 1;
ReadIn (G, Newsence);
WriteIn      (Device, Newsence);
If screen  = S then
Begin
WriteIn      (" type  < space >  to continue') Read (space);
end;
End;
Close (f); close   (G, lock);
End;
Write (Type <space> to continue") read (space);
End
Until (decision □ ◻"E" ) and decision □ ◻'D' ) and Decision < > T );
Close = Device, lock;
End.
```

CHAPTER 5

5.1 SUMMARY AND CONCLUSIONS

The application package which does not need special user training has been developed. The package which was developed could serve different specialist and serves as practical and theoretical tools for security planning in computing activities.

Since the aim of the project is to maintain privacy and security of data. The package is able to fully secure the data in the system.

Meanwhile it is better to note that no system is fool proof because the issue of security in computing is h highly dynamic. With this reason, some area of suggestion for further research would be suggested.

One area which has not been explore but which is a thorough research is done will go a long way in alleviating data security problem is **SYSTEM SURVEILLANCE**. The technique involves the building of surveillance or detective reputing into the system in order to identify attempted violates.

Another important aspects of security which has been handling with nonchalant attitude is the contingency and incident handling in most organization. It is discovered that most of the organization lacks contingency planning that is if there is an accident or virus invasion into the system, this is an area for further research for any interested researcher.

It is better to consider the warning of Artemiderous to the Great Julius Caesar in one of the Shakespear plays that "Security gives way to conspiracy". This warning becomes necessary because no matter how effective a security is, it becomes ineffective when the threat come from within. Therefore a high degree of motivation in form of monetary and other incentives which promote job contentment in staff is suggested computer experts in an organization should be highly remunerated to dissuade them from participating in fraudulent practices.

look simple but will be very effective if more research is done. The mainstream of the technique is that organization should have different rather than one enciphering technique. Each technique employed should have a code. This will make enciphering technique more complex thereby reducing the chance of breaking the code.

The final achievement of effective security measure requires all personnel to be aware and committed to constant improvement and central surveillance on day to day basis.

BIBLIOGRAPHY

(1) ALEXANDER, M. ed. "Multimedia Means Greater Awareness" In fosecurity News 4(6), 1993 pp 90-94

(2) BURNS, G. M "A Recipe for a Decentralized Security Awareness program" 1SSA Access Vol 3, Issue 2, 2nd Quarter 1990 pp 12-54

(3) FITES, P. AND M. KRATZ Information Systems Security: A Practioner's Reference. New York, NY: Van Nostrand Reinhold, 1993.

(4) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "Security issues in Public Access Systems". Computer System Laboratory Bulletin. May 1993.

(5) NORTH S. "To Catch a 'Crimoid," Beyond Computing (1), 1992. pp 55-56.

(6) PANKAU, E. "The Consumate Investigator" Security Management. 37(2), 1993. pp. 37-47.

(7) SINKOV ABRAHAM Elementary Cryptoanalysis. Mathematical Association of America 1996.

(8) MARTIN JAMES Security Accuracy and Privacy in Computer System. Prentice-Hall Inc. New Jersey 1973.

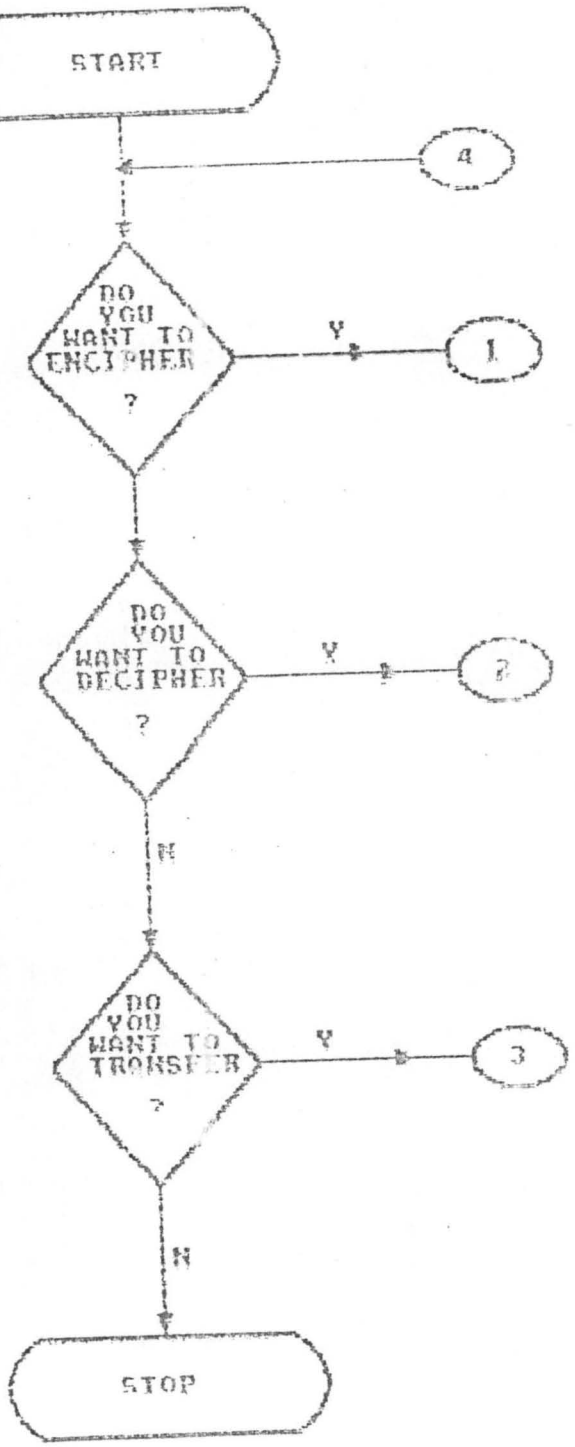
(9) DAVID LIGHTFOOT Computer Programming in Pascal Richard Clay Ltd Bristol - 1983.

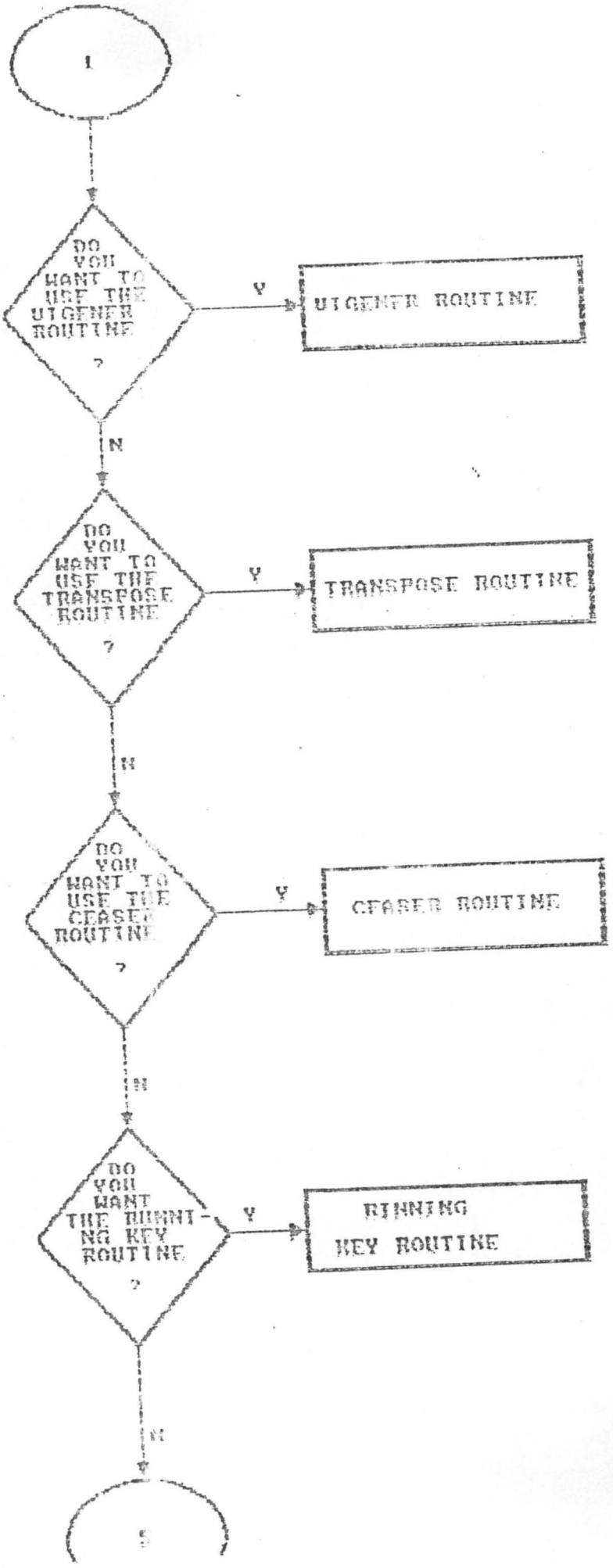
(10) BROWNE PETERS 'Computer Security - a survey " New York 1972.

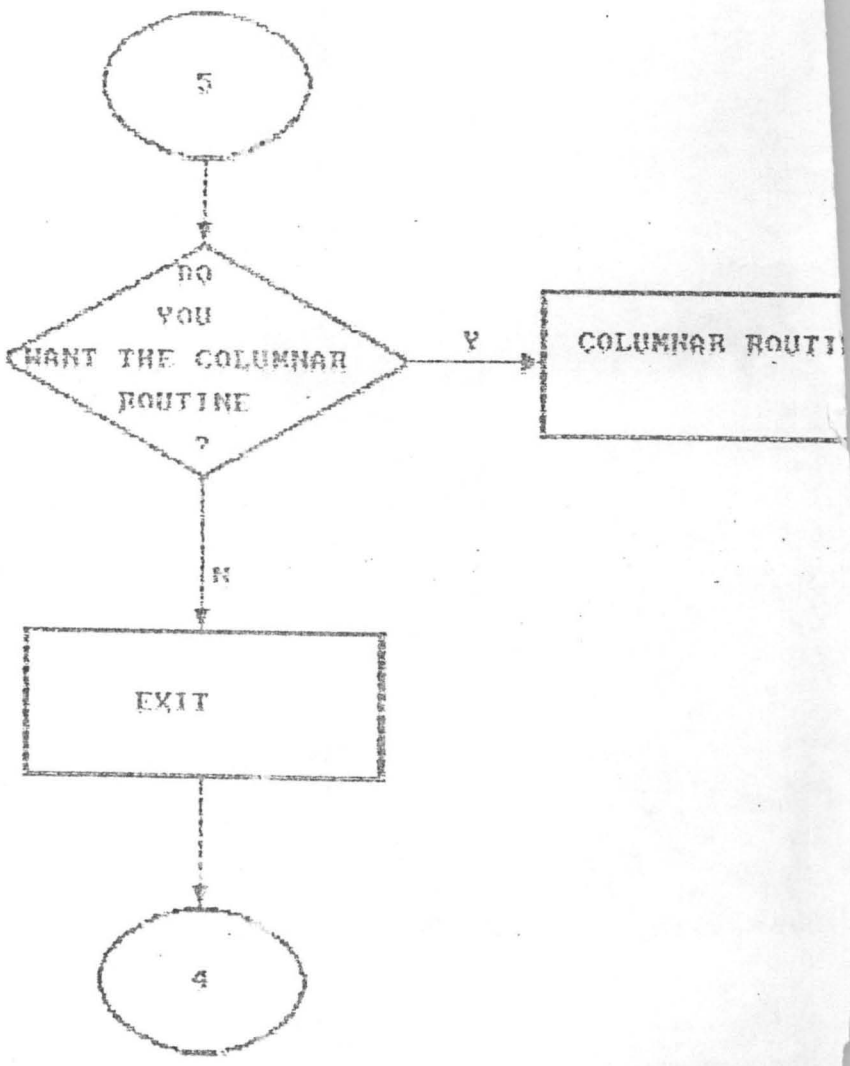
(11) DON B. PARKER Threats to Computer System. The Risos Project March 1973.

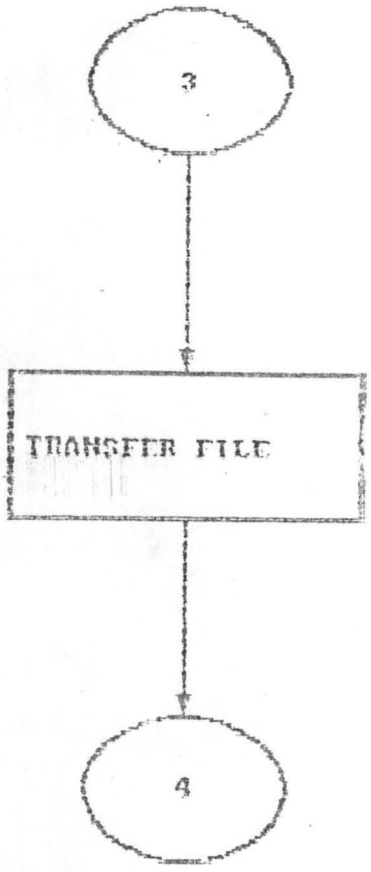
(12) ALLEN B. R. " Danger Ahead! Safeguard your Computer Vol 12, Academic Press Inc. New York 1972.

FLOWCHARTS


START
4
DO YOU WANT TO ENCIPHER ?
Y
1
DO YOU WANT TO DECIPHER ?
Y
2
N
DO YOU WANT TO TRANSFER ?
Y
3
N
STOP


1
DO YOU WANT TO USE THE UIGENER ROUTINE ?
Y
UIGENER ROUTINE
N
DO YOU WANT TO USE THE TRANSPOSE ROUTINE ?
Y
TRANSPOSE ROUTINE
N
DO YOU WANT TO USE THE CEASER ROUTINE ?
Y
CEASER ROUTINE
N
DO YOU WANT THE RUNNING KEY ROUTINE ?
Y
RUNNING KEY ROUTINE
N
5


5
DO
YOU
WANT THE COLUMNAR
ROUTINE
?
Y
COLUMNAR ROUTI
N
EXIT
4


3
TRANSFER FILE
4