**CHAPTER ONE**

**INTRODUCTION**

**1.1 Background of study**

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

One of the techniques of one of achieving this purpose is “Cryptography”. Cryptographic techniques have been used to protect information since ancient times, but only individuals and organizations with extraordinary need for confidentiality like the military government had bothered to exert the effort required to implement it. But as time passed and information security grew larger due to everyday businesses, cryptography became one of the most important tools for privacy and also a means of access control or restriction.

One basic topic in cryptography is that of Encryption and Decryption. Encryption is defined as the conversion of information\*written, readable text) to an unreadable form called cipher text, which is impossible to read except of those that posses the secret key or appropriate knowledge to decipher the message. Decryption on the other hand is the opposite of Encryption that is the transformation of the cipher text back to its original form. The process of Encryption and Decryption require the use of secret information called the key. Cryptography is one practical means of sending information over an insecure channel. These channels may be computer networks, telephone lines, wireless intercom system, internet, bank ATM etc.

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

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

**1.2 Statement of Problem**

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

1.3 Aim of the Study

The aim of the study is to design and implement a computerized data encryption system for military staffs of Nigerian Police Force.

**1.4 Objective of the Study**

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

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

**1.5 Scope of the Study**

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

**1.6 Significance of the Study**

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

**1.7 Limitation of the Study**

Limitations encountered during this project study include:

* Lack of good text and journals on cryptography
* Inadequate finance
* Time constraint

**1.8 Definition of Terms**

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

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

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

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

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

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

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

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

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

**CHAPTER TWO**

**LITERATURE REVIEW**

## 2.1 INTRODUCTION

Data encryption has gradually developed since ancient times and many different forms of encryption keeps formulating. Some are extension of others while some are new forms entirely. In either case, the encryption method can be either substitution or a transposition. And either a block or a stream.

There are numerous studies and applications that have been designed specifically for data encryption. This chapter makes a review on how cryptography stated in ancient times and also makes a review of the system security cryptography in .Net framework and the c# programming language which is going to be used in writing the codes for the software in this research work/project.

## 2.2 WHAT IS CRYPTOGRAPHY AND CRYPTANALYSIS?

Cryptology is the study of both **cryptography** and **cryptanalysis**, or the breaking of coded messages. It is nearly as old as civilization itself, although ciphers and codes prior to the late middle ages period in Western Europe tended to be extremely simple by today's standards. Early examples of cryptology can be found in the work of Mesopotamian, Egyptian, Chinese, and Indian scribes. In those four cradles of civilization, which emerged during the period between 3500 and 2000 B.C., few people could read and write, therefore, written language was a secret code in itself. Further concealment of meaning behind opaque hieroglyphs, cuneiform, or ideograms served to narrow the intended audience even further.

Cryptography is one of the oldest fields of technical study we can find records of, going back at least 4,000 years ago. The development of cryptography began from the need to maintain personal, political or military secrecy back in the days. It was to prevent this sort of leakage of information that the Egyptians, the Greeks and so on developed various forms of secret writing and the Romans experimented with both invisible ink and the substitution ciphers.

**2.2.1 HISTORY OF CRYPTOGRAPHY/ CRYPTANALYSIS**

Cryptography probably began in or around 2000 B.C. in Egypt, where hieroglyphics (a writing system using picture symbols; used in ancient Egypt) were used to decorate the tombs of deceased rulers and kings. These hieroglyphics told the story of the life of the king and proclaimed the great acts of his life. They were purposefully cryptic, but not apparently intended to hide the text. Rather, they seem to have been intended to make the text seem more regal and important. As time went by, these writings became more and more complicated, and eventually the people lost interest in deciphering them. The practice soon died out. (Cohen, 1995)

The ancient Chinese used the ideographic nature of their language to hide the meaning of words. Messages were often transformed into ideographs for privacy, but no substantial uses in early Chinese military conquests are apparent. Genghis Khan, for example, seems never to have used cryptography.

The Spartans used a system which consisted of a thin sheet of papyrus wrapped around a staff. Messages were written down the length of the staff and the papyrus was unwrapped. In other to read the message, the papyrus had to be wrapped around a staff of equal diameter. It is called the ‘skytale’. And was used in the 5th century B.C. to send secret messages between greek warriors. Without the right staff it would be difficult to decode the message using the techniques available at that time.

In India, secret writing was apparently more advanced, and the government used secret codes to communicate with a network of spies spread throughout the country.

**2.2.2 THE RELEVANCE OF CRYPTOGRAPHY TO SECURITY INFORMATION**

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptography key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signature, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more applications such as that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email. Cryptography solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

## 2.3 BRANCHES OF CRYPTOGRAPHY

**I.) Substitution**

This branch of cryptography involves substituting each letter in the plaintext with a different letter. The units of the plaintext are replaced with ciphertext according to a regular system. The units may be single letter (the most common), pairs of letters, triplets of letters or mixtures of the above. The receiver deciphers the text by performing an inverse substitution.

“A substitution technique is one in which letters of the plain text are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns” (Stallings, 2005)

“In substitution, the letters of the plaintext are replaced by other letters or by numbers or symbols. Thus secret might become 19 5 3 18 5 20 or XIWOXY in a more complicated system.” (Khan, 1967)

**II.) Transposition**

The letters of the message are simply rearranged. Transposition techniques typically transposes the position of the plaintext elements. The simplest of this technique is referred to as the “Rail Fence Technique” in which a plaintext (message to be encrypted) is simply written down as a sequence of diagonals and then read off in rows.

In **transposition,** the letters of the plaintext are jumbled; their normal

Order is disarranged. To shuffle *secret* into ETCRSE is a transposition. The letters retain their identities, the two e's of *secret* are still present in ETCRSE but they lose their positions (Kahn, 1967)

The way in which the plain text is processed into the ciphertext (encrypted message) can be either **block** or **stream**.

Block ciphers process messages in blocks, each of which is then encrypted or decrypted. E.g. is the Digital Encryption standard (DES) Stream ciphers process messages a bit or byte at a time when encrypting or decrypting. Example is a system security cryptography in .Net Framework.

## 2.4 BRIEF HISTORY OF C#

C# (pronounced as see sharp) is a Multi-paradigm programming language encompassing strong typing, imperative , declarative ,functional, generic, object-oriented (class-based), and component-oriented programming disciplines. It was developed by Microsoft within its .NET initiative and later approved as a standard by Ecma (ECMA-334) and ISO (ISO/IEC 23270:2006). C# is one of the programming languages designed for the Common Language Infrastructure.

C# is a general-purpose, object-oriented programming language. Its development team is led by Anders Hejlsberg. The most recent version is C# 7.0 which was released in 2017 along with Visual Studio 2017.

## 2.5 REVIEW ON SYSTEM SECURITY CRYTOGRAPHY IN C#

## The System Security Cryptography namespace provides cryptographic services, including secure encoding and decoding of data, as well as many other operations, such as hashing, random number generation, and message authentication. For more information, see Cryptographic Services.

**CLASSES:**

**.Net Framework** has numerous amounts of classes in the system security cryptography but we will highlight the crypto classes that was used during the building of the project which are:

**MD5 :** Represents the abstract class from which all implementations of the MD5 hash algorithm inherit.

**SHA1:**which Computes the SHA1 hash for the input data.

### 2.6 Features of C#

January 1999, Anders Hejlsberg, C# is simple, object oriented, distributed, interpreted, robust, secure, architecture neutral, portable, high performance, multithreaded, and dynamic”

* **Functional programming**

Though primarily an imperative language, C# 2.0 offered limited support for functional programming through first-class functions and closures in the form of anonymous delegates. C# 3.0 expanded support for functional programming with the introduction of a lightweight syntax for lambda expressions, extension methods (an affordance for modules), and a list comprehension syntax in the form of a "query comprehension" language.

* **Object Oriented**

C# is intended to be suitable for writing applications for both hosted and embedded systems, ranging from the very large that use sophisticated operating systems, down to the very small having dedicated functions.

* **Distributed**

Internet programmers can call functions on these protocols and can get access to the files from any remote machine on the internet rather than writing codes on their local system.

* **Boxing and unboxing**

Boxing is the operation of converting a value-type object into a value of a corresponding reference type. Boxing in C# is implicit.

Unboxing is the operation of converting a value of a reference type (previously boxed) into a value of a value type. Unboxing in C# requires an explicit type cast. A boxed object of type T can only be unboxed to a T (or a nullable T).

Example:

int foo = 42; // Value type.

object bar = foo; // foo is boxed to bar.

int foo2 = (int)bar; // Unboxed back to value type.

* **Secure**

C# is meant to be used in networked environments therefore access restrictions are enforced (public, private and protected).

* **Property**

C# provides properties as syntactic sugar for a common pattern in which a pair of methods, accessor (getter) and mutator (setter) encapsulate operations on a single attribute of a class. No redundant method signatures for the getter/setter implementations need be written, and the property may be accessed using attribute syntax rather than more verbose method calls.

* **Portable**

By design, C# is the programming language that most directly reflects the underlying Common Language Infrastructure (CLI). Most of its intrinsic types correspond to value-types implemented by the CLI framework. However, the language specification does not state the code generation requirements of the compiler: that is, it does not state that a C# compiler must target a Common Language Runtime, or generate Common Intermediate Language (CIL), or generate any other specific format. Theoretically, a C# compiler could generate machine code like traditional compilers of C++ or Fortran.

* **High Performance**

C# is an interpreted language; in fact, it is about 20 times as slow as C. However, this speed is more than enough to run interactive, GUI and network-based applications, where the application is often idle, waiting for the user to do something, or waiting for data from the network.

* **Dynamic**

C# was designed to adapt to an evolving environment. C# loads in classes as they are needed, even from across the network. It defers many decisions (like object layout) to runtime, which solves many of the version problems that C++ has.

**CHAPTER THREE**

**RESEARCH METHODOLOGY**

3.1 OVERVIEW OF THE EXISTING SYSTEM

This chapter describes the existing system which is manually carried out where information on military signals is stored in an office file. Their personal data are being collected and each person has a file created for him or her. This files are mostly written in plain text which makes them vulnerable to attackers, hence there is need for the implementation of an information encryption system.

**3.2 FACT FINDING METHOD**

Different methods adopted in the collection and gathering Data and Information for the project include Reference to written texts.

**3.2.1 REFERENCE TO WRITTEN TEXT**

Security information documentations were studied and a lot of information concerning the system in question was obtained. Some forms that are necessary and available were assessed. Also internet downloads was made to obtain some text materials.

**3.2.2 ORGANIZATIONAL STRUCTURE**

**INSPECTOR GENERAL OF POLICE**

**AIG ZONE 1**

**POLICE**

**CO**

**M**

**MISSIONER**

**IMO**

**SATE**

**POLICE**

**COM**

**M**

**ISSIONER**

**ENUGU S**

**T**

**ATE**

**POLICE**

**COM**

**M**

**ISSIONER**

**ANAMBRA**

**S**

**T**

**ATE**

**POLICE**

**CO**

**M**

**MISSIONER**

**ABIA**

**S**

**T**

**ATE**

**AIG ZONE 3**

**AIG ZONE 6**

**AIG ZONE 2**

**AIG ZONE 4**

**AIG ZONE 5**

**POLICE**

**CO**

**M**

**MISSIONER**

**EBONYI**

**SATE**

**ASSISTANT**

**CO**

**M**

**MISSIONER OF**

**POLICE**

**DEPUTY POLICE**

**CO**

**M**

**MISSIONER**

**DEPUTY POLICE**

**CO**

**M**

**MISSIONER (CRIME)**

**OTHER OFFICERS**

**DIVISIONAL POLICE**

**OFFICER**

**DIVISIONAL OFFICER IN**

**COMMAND**

**FIGURE 3.1** ORGANIZATIONAL STRUCTURE OF INFORMATION FLOW IN NIGERIA POLICE FORCE

**3.3 OBJECTIVES OF THE EXISTING SYSTEM**

The objective of the existing system includes:

* Collection of police personnel information
* Opening a file for documenting these information
* Storing in a cabinet or server

**3.4 INPUT, PROCESS AND OUTPUT ANALYSIS**

**3.4.1 INPUT ANALYSIS**

The input to the system is the security information form. This form is used for recording security signals this forms the input to the system.

**3.4.2 PROCESS ANALYSIS**

The information gathered was processed into a more meaningful format for entry into the system. These personnel data are processed to find out their areas of specialization and signal information sent out.

**3.4.3 OUTPUT ANALYSIS**

The output from the system is generated from the system inputs. More of the output generated is on personnel record, military signals, etc.

**3.5 PROBLEMS OF THE EXISTING SYSTEM**

Manual system of operation faces a lot of problems which includes:

* High exposure of sensitive information
* Vulnerable to attackers
* Loss of materials on transit Insecurity of data

**3.6 SYSTEM ANALYSIS**

The purpose of this phase is to understand how the Advanced Encryption Standard encryption/decryption works manually. This can however lead to successful design of the software.

### 3.6.1 The Advanced Encryption Standard (AES/Rijndael)

The Advanced Encryption Standard (AES) also known by its original name Rijndael (Dutch pronunciation: [ˈrɛindaːl]), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.it is the current encryption standard intended to be used by U.S. Government to protect sensitive information.

A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. ... Two of the most common hash algorithms are the MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm).

The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

### 3.6.2 The Hash Algorithm

The Hash algorithm are used in so many ways. The most common are as follows:

**MD5**: The key is random, so the ciphertext too will be completely random. Hence it is impossible to recover the original message without the appropriate key.

Suppose we want to encrypt a message SECRET and our randomly generated key is FXIPUF.

## 3.7 SYSTEM DESIGN

The proposed application program is to implement the encryption and decryption of the AES (Advanced Encryption Standard) using C# programming Microsoft Visual Studio. The program’s source code is presented in Appendix A, as such some part of it will be referenced in this chapter. The program will have the following features present:

* A graphical user interface using ASP.Net and Materialize css. It will be used in creating the side-navigation, image slider, dropdowns, input/output text areas, buttons, containers, etc.
* The first instance of the program will provide the user with a login page to login as the system software administrator
* The login button leads the user to another interface know to be the dashboard.
* The second interface of the program which is the dashboard consists of (1)a side-navigation bar with five active links which are :Home, Data Encryption, Data Decryption , About and Logout
* In the home we have 2 components (1) an image slider (2) a collapsible bar
* If we navigate to the Data Encryption link we have a simple container that consists of :

1. A plain-text input area where we type our plain text or paste data information
2. A dropdown bar where we choose our encryption method i.e MD5 or SHA1
3. An encrypt button which converts plain text to cipher text in desired encryption that was selected
4. A output which is an uneditable text input area where our cipher text is produced

* If we navigate to the Data Decryption link we also have a simple container that consists of :

(1) An encrypted-text input area where we paste our cipher text received.

(2) A dropdown bar where we choose our encryption method that was used to encrypt the text i.e. MD5 or SHA1

(3) A decrypt button which converts cipher text to plain text.

(4) An output which is an uneditable text input area where our plain text is produced

* The about page which contains information about the application.
* The logout link which signs out and closes application sessions.

### 3.7.1 DATA FLOW DIAGRAM (DFD)

To have a clear picture on how the automated system works, a data flow diagram (DFD) is shown below. The diagram will show how data is processed by the system in terms of inputs and outputs.

USER

Inputs message

Random key

Return encrypted message to user

**Figure 3.2: DFD 1: ENCRYPTION**

USER

Inputs the ciphertext

Plaintext Alphabets

Returns plaintext to user

**Figure 3.3: DFD 2: DECRYPTION**

**3.8 JUSTIFICATION FOR THE NEW SYSTEM**

The new system will help to solve all the problems inherent in the existing system. The justification for the new system includes:

* Reduction of unauthorized access
* Enhance information integrity
* Security of information is guaranteed

## 3.9 SYSTEM SPECIFICATION

This application software program is a graphical user interface (GUI) application program and also a standalone application that has three forms. The software program also provides some of the necessary options for encryption and decryption, or both of a given message. The software needs the following hardware and software specifications.

**Hardware Specification**

For the program to run successfully, it requires the following list of items:

* + At least 2GB of RAM (Random Access Memory) and
  + A processor of at least one (1.5) GHZ. Or higher

**Software Specification**

For the system to run effectively, it also requires the following software specifications:

* Visual Studio 2015 or higher version
* Windows Operating System
* .Net Framework 3.5 or higher version
* Google chrome or any other web browser

**CHAPTER FOUR**

**SYSTEM IMPLEMENATION, RESULT AND TESTING**

**4.1 SYSTEM IMPLEMENTATION**

The purpose of system implementation can be summarized into two functions; namely making the system available to end users (the deployment), and positioning on-going support and maintenance of the system with the performing organization (the transition). At a finer level of detail, deploying the system consists of executing al steps necessary to educate and train the end users on the use of the proposed system, placing the proposed system into production, confirming that all data required at the start of operations are available and accurate and validating that business functions that interact with the system are functioning properly.

**4.2 ACCESSING THE APPLICATION FROM A WEB SERVER**

Accessing is the process of making use of programs that is uploaded to a web server. The following procedure should be followed when accessing the application:

* Go to the specified webpage its uploaded eg.www.IDE.com
* The page will automatically show a “user login Screen” on the browser prompting for user ID and password. Type “Admin” as user ID and “admin123” as the default user ID and password.

**4.3 FLOW CHART OF THE SYSTEM**

LOG IN

DATA ENCRYPTION

CIPHER TEXT

DATA DECRYPTION

PLAINTEXT

4.1 Flow chart of the System.

## 4.4 PROGRAM DOCUMENTATION:

The designed system has three forms: The following are the steps for encryption and/or decryption process:

**Step 1:** Run the program by clicking on the start command from the Visual studio or by clicking on F11 function key on your keyboard as below:

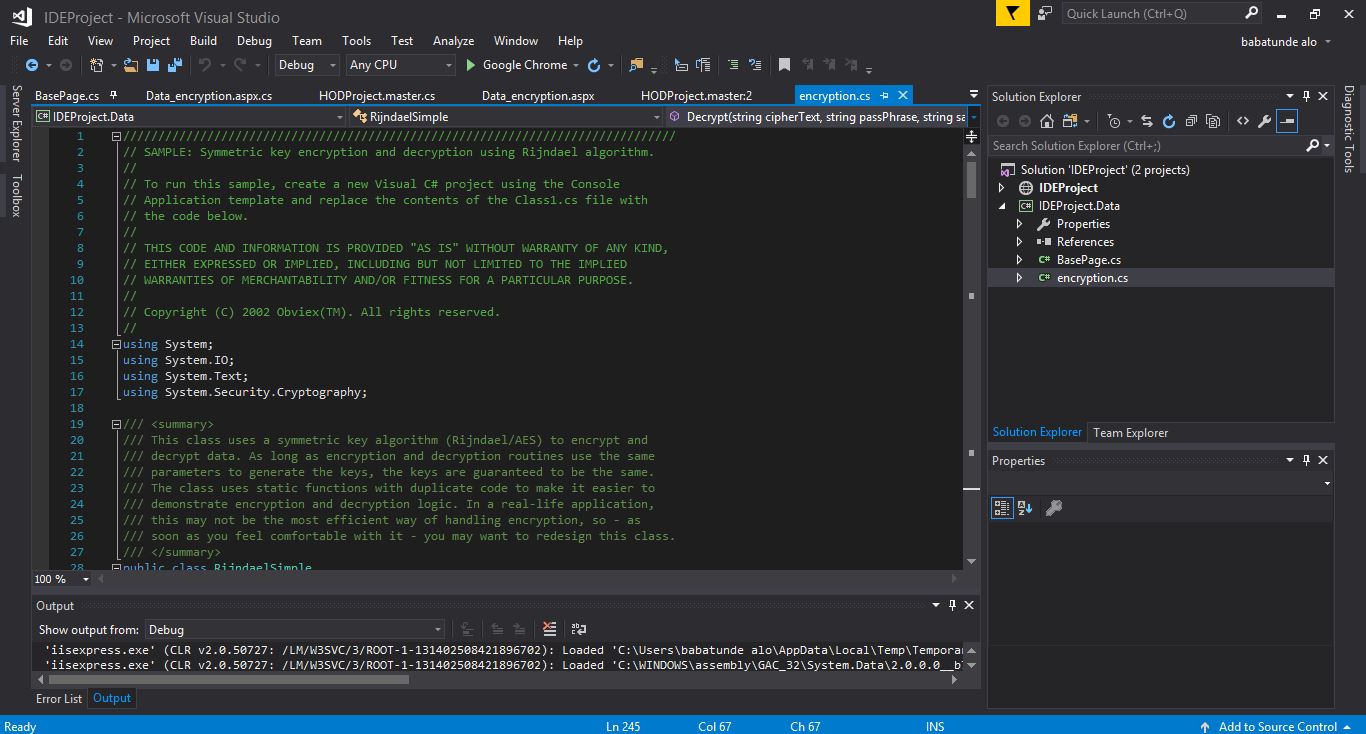


Figure 4.1 Application IDE

**Step 2:** The main program window will be displayed. Then provide the login parameter where username is “admin” and the password is “admin123” as in Figure below:

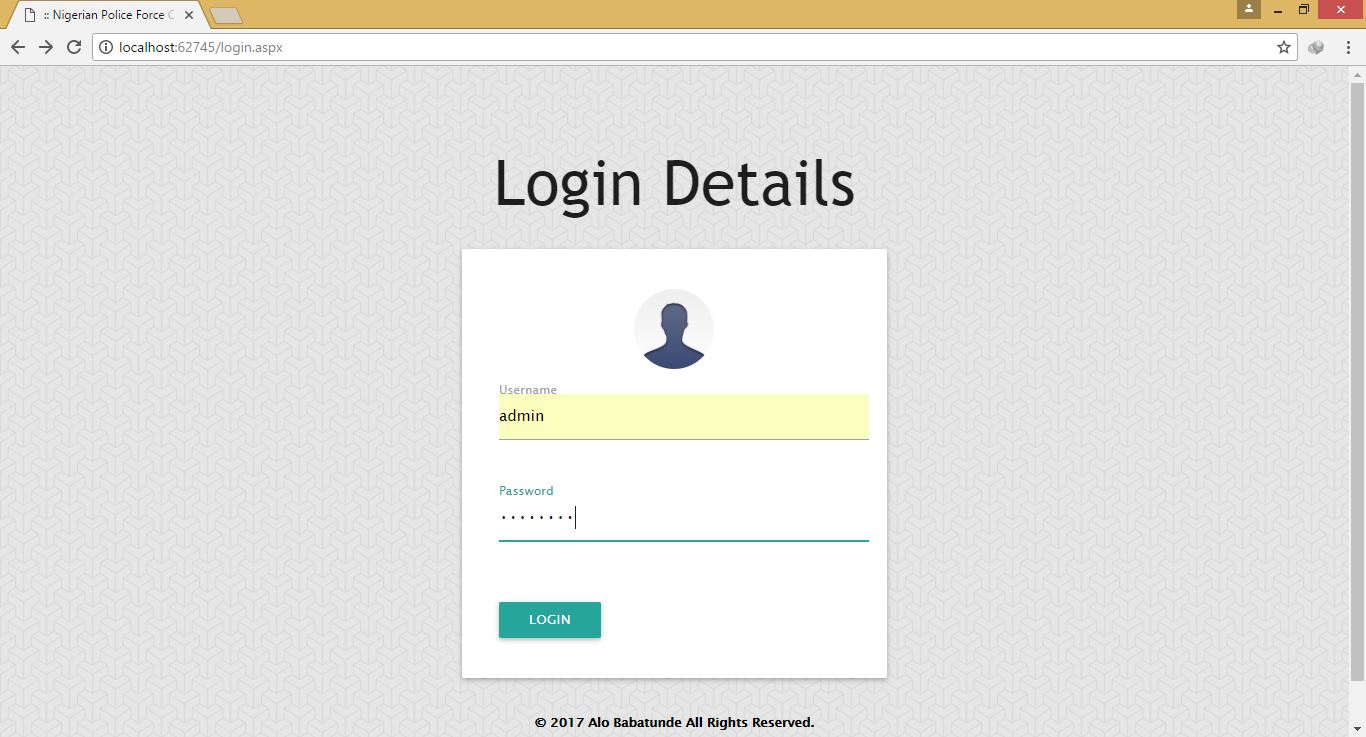


Figure 4.2 Login Page

**Step 3:** The home window will be displayed. Which contains an image slider and a collapsible bar at the button which displays the aim of the software area as below:

****

Figure 4.3 Home Page

**Step 4:** Then clicking on the data encryption button opens an encryption window that displays. A text area is displayed to type the message as below:

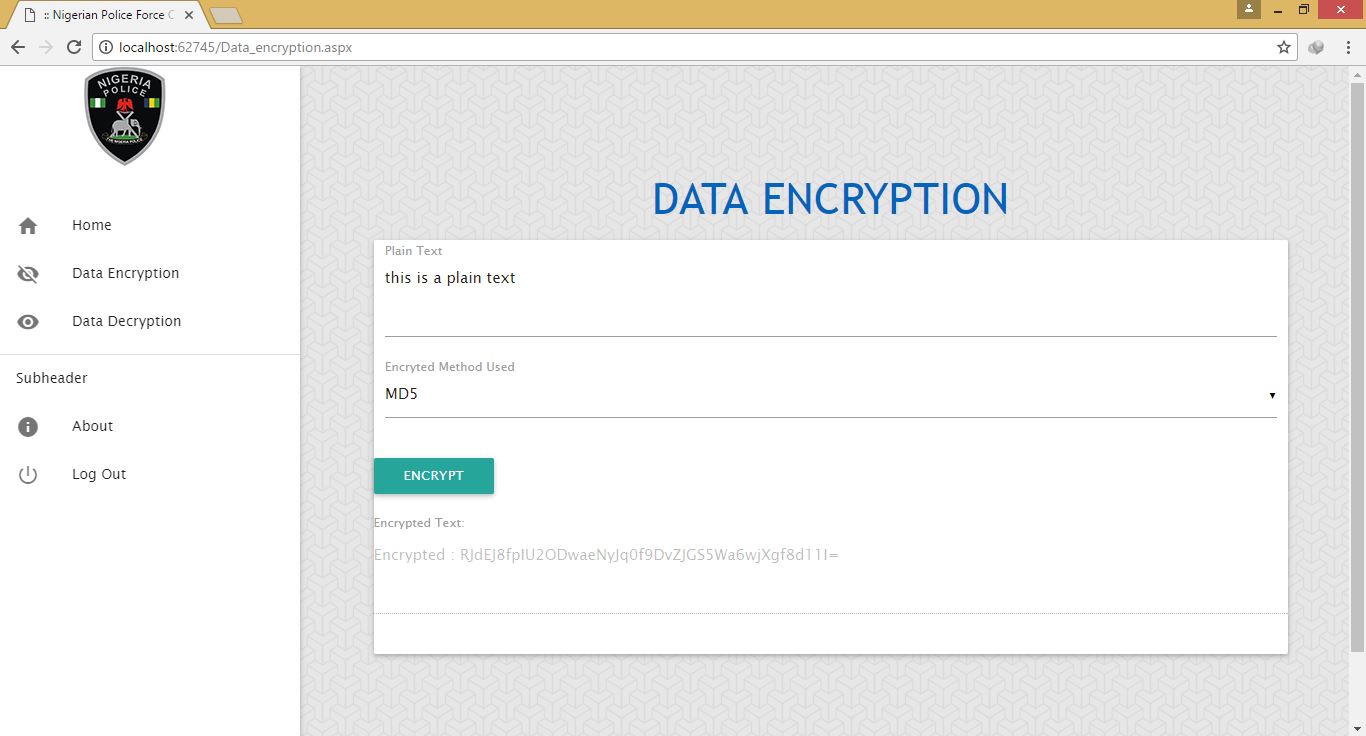


Figure 4.4 Data Encryption Page

**Step 5:** Copy the cipher text that was generated and paste in the data decryption form:

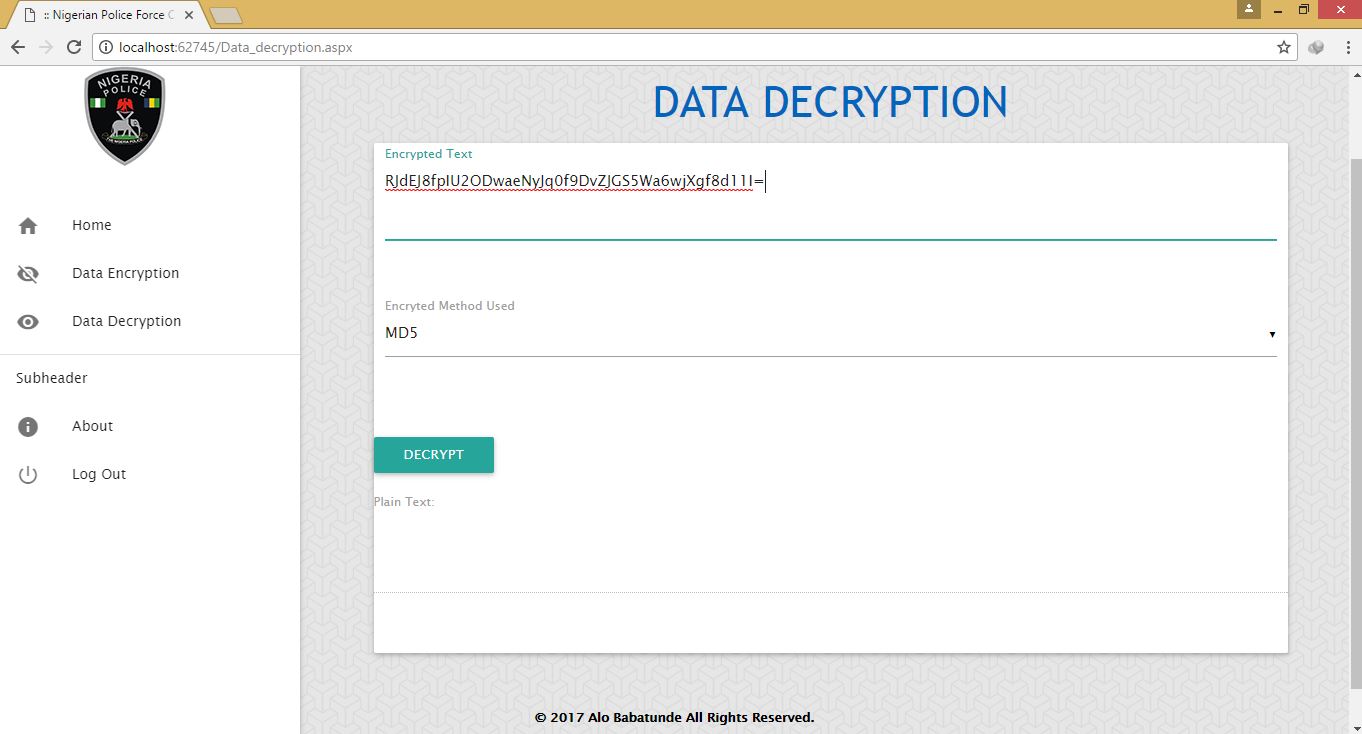
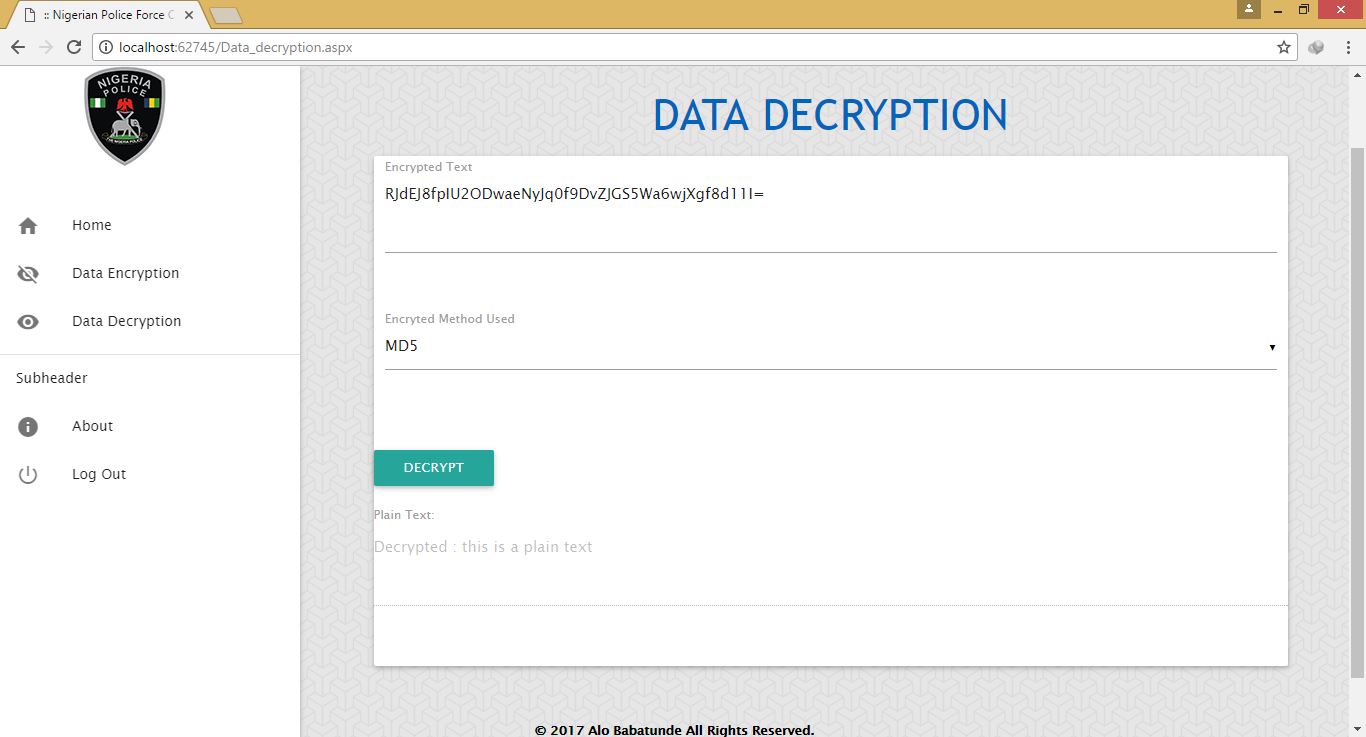
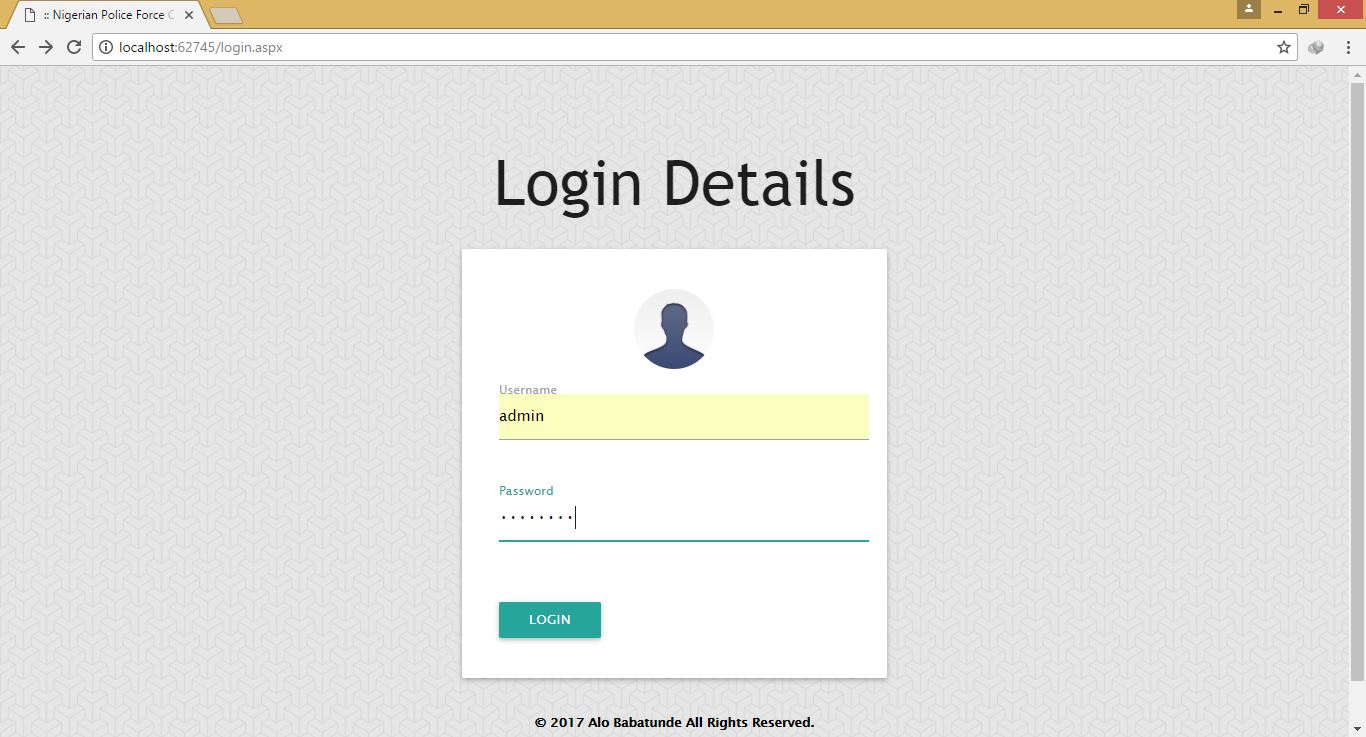


Figure 4.5 Data Decryption Page

**Step 6:** Clicking on the encrypted method choose the method used in encrypting the plain text then click on the decrypt button as shown below:



**Step 7:** clicking on the logout button then exits the application window.

****