FACULTY OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY OF MALAYA
KUALA LUMPUR

Perpustakaan SKTM

CIPHERCRYPT-AN ENCRYPTION SYSTEM

By

NOR HIDAYAH NGAH
(WEK 990445)

Under The Supervision Of

MRS. FAZIDAH OTHMAN

SESSION 2003/2004

A PARTIAL FULLFILMENT FOR THE BACHELOR DEGREE OF COMPUTER SCIENCE

University of Malaya

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

University of Malaya

CHAPTER 3- SYSTEM METHODOLOGIES

CHAPTER 4-SYSTEM DESIGN

CHAPTER 5-SYSTEM DEVELOPMENT & IMPLEMENTATION

University of Malaya

CHAPTER 6-SYSTEM TESTING

CHAPTER 7-CONCLUSION

University of Malaya

LIST OF FIGURES

University of Malaya

ACKNOWLEDGEMENT

~~In memory of my beloved parent, Allahyarham Ngah b. Daud and Allahyarhamah Fatimah bt. Omar. May their soul rest in eternal peace. Ameen~~

Firstly, I would like to express my heartfelt gratitude to my project supervisor, Miss Fazidah Othman I unequivocally appreciate your guidance, patience and cooperation given . A word must also said to my project moderator, Miss Laiha Mat Kiah and Mr. Amirrudin Khamsin for spending time evaluating me during viva sessions and also for the feedback for this project.

My heartiest thanks goes to all my family members; my 5 sisters and 4 brothers for their endless moral support & always there when I needed them. To my friends who've helped me a lot through the hard time of this project and whose comments have helped shape this report, a big thanks to all of them. All their names may not appear in this report but whose idea and advice were crucial to the success of my project report.

Lastly, to whom I failed to mention, a bunch of thanks to all and everyone of them. Thank you.

ABSTRACT

Ciphercrypt is a stand-alone system focused on providing basic introduction and idea of cryptography implementation to people who are without knowledge and not very familiar with the art of cryptography. This system is implemented on a Windows platform with Visual Basic as a programming language and 3-DES as a main encryption algorithm.

By using Ciphercrypt, users can encrypt and decrypt their data as they wanted by simply clicking the encrypt / decrypt button. There are 3 types of encryption algorithm provided which are 3-DES , RC4 and RC2. Users need to input any keyword and choose any of the 4 types of keyword hash function which are MD5, MD4, MD2 and SHA-1 . Different keyword used will produce a different encrypted / decrypted output.

The hashed keyword will be used in encrypt / decrypt process by using any of 3 encryption algorithm mentioned before. The decrypted / encrypted message can be view in Window Notepad and both of the files are automatically created after the encrypt / decrypt process.

It is hoped that this system will be further developed in the future to explore more functionalities with added enhancements and widen the target group scope.

University of Malaya

1.0 INTRODUCTION

1.1 OVERVIEW

The internet is becoming a primary source for information. The amount of the information is so overwhelming that users can spend hours and hours browsing the internet. More and more companies do business by sending data in the form of email over the internet. As information becomes an increasingly commodity, and as the communications revolution changes society, so the process of encoding messages known as encryption will play an increasing role to in everyday life.

Nowadays our e-mails pass through various computers and this form of communication can be intercepted with ease, so jeopardizing our privacy. More and more companies do business by sending data in the form of email over the internet. Since we are moving toward a future where the nation will be crisscrossed with high capacity fiber optic data networks linking together all our increasingly ubiquitous personal computers, encryption is the only way to protect our privacy and guarantee the success of the digital marketplace. The art of secret communication, otherwise known as cryptography, will provide the locks and keys of the Information Age.

Without paper precautions, personal computer and private networks are exposed to security threats such as eavesdropping, modification, and impersonation making their private and sensitive information totally vulnerable to computer hacker. Therefore, internet security becomes very important to every user. One of the internet security method is data encryption.

Encryption is said to be the most effective security method on the internet. It works like a clock that requires a specific key to open it. Encryption keeps data secure during transmission over internet while it is being stored in a computer. A good encryption system will protect and secure to be good and be able to sustain attack from computer hackers. It has to have to a strong encryption algorithm.

Therefore with data security being the main concern at hand, this project will undertake to a good and strong encryption system. This encryption system will be name as 'Ciphercrypt'.

1.2 OBJECTIVES

The objectives of this projects are as follows:-

1. This system's main objective is to give a chance for different levels of users to get to know about this encryption system and aware of security threats not only on online transactions but also for personal use such as for undergraduate students and small local companies since all other product's target user are only for international and corporate companies.

2. To design and develop a symmetric encryption with a strong encryption algorithm (3-DES) that will provide secrecy and data integrity. Secrecy refers to the concealment of information. Therefore, with secrecy the user will be able to store important and private information without the fear of it being read by other than intended reader. Providing data integrity means to ensure that the information stored /sent will not be attacked, changed or tampered by a computer hacker on an unauthorized person.

3. To design and develop a simple but attractive interfaces to make Ciphercrypt a user-friendly one.

4. To design and develop a system that will enable the user to secure their data not only during email transmission but also for personal references.

5. To design and develop a user verification feature to protect the system itself from unauthorized users.

University of Malaya

1.3 SCOPE

Ciphercrypt is going to be a stand-alone symmetric encryption system using. It is symmetric because the one key will be used for encryption and decryption of the data . The user will be asked for their username and password before login to our system. A keyword, type of encryption algorithm and keyword hash function to be used are required before the system can encrypt the file or data. This system will be able to encrypt and decrypt all ASCII standards character. These are the detail scope of Ciphercrypt system:

<u>Phase 1: Authentication Session</u>

During the authentication session, the user will be asked to enter a user name and password before proceeding to the main screen. To proceed, both the required details must be correct.

<u>Phase 2: Encryption / Decryption</u>

In Ciphercrypt, users can choose to only encrypt file and decrypt it later or encrypt/ decrypt file at the same time. The encrypted / decrypted output files are automatically created and can be retrieved at the same path with the original file. The output can be viewed at any time just by choosing any of existing file, click the encrypt/decrypt buttons and view button for a bigger output screen.

University of Malaya

1.4 SIGNIFICANCE OF THE PROJECT

Ciphercrypt will have an interface that will meet the requirements and the characteristics of the liking of the user. The characteristic of the interface will be as follows:

1. Attractive

The interface will have a creative and unique design with suitable and matching colors to complement it.

2. User Friendly

The interface will also have an easy to use features and it will be informative so the user will be able to use the system with ease without hassle or confusion.

3. Reliable

Besides the cosmetics, Ciphercryp will provide a strong and complex encryption and decryption algorithm which is the very basis and core of the system.

University of Malaya

A Ciphercryp will provide a help option to assist the new user in using the application or matters regarding cryptography . This option will include:

1. User Manual

The user manual will have a step by step guide on how to use Ciphercrypt. This will be useful to a user if a problem or confusion were to arise during or before using the application.

2. List of Definations

To provide definations of terms related to cryptography for the user's reference.This will help improve the knowledge of the user as well as giving a better overall understanding on Ciphercrypt.

3. User Verification

Last but not least, Ciphercrypt will provide a user verification function. The purpose of this is to only permit/allow an authorized person to use the system.

University of Malaya

1.5 PROBLEMS OF EXISTING SYSTEM

1. The majority of email users today do not use any method of encryption, giving little opportunity for using it on a regular basis to stay familiar with it.

2. Cryptography is a foreign concept for most people, and keeping up with keys, pass phrases, and trust can be overwhelming for the casual user. The use of encryption for email has not been widely adopted, mainly due to a lack of knowledge about the subject, and users not being aware of the need for it. For some, the concept is only as good as the software they can use to implement it, and getting up to speed with Internet browsing and email are difficult enough without introducing another concept, more software to install, things to remember, etc.

3. Bad press relating to how encryption technology such as Pretty Good Privacy (PGP) has been used in plotting terrorist attacks (a major point of contention, the debate of which is on-going).

4. The encryption products are very expensive resulting user and small companies not interested on trying/ buying the products.

University of Malaya

1.6 HARDWARE & SOFTWARE REQUIREMENTS

1.6.1 Hardware Requirements

The requirements needed to execute or run Cypercrypt requires only minimal spec of an average computer , these are as follows:

1. All standard peripherals of a computer such as a monitor, keyboard, mouse, etcetera
2. At least Pentium I or any equivalent microprocessor
3. Minimum of 32 Mb RAM is recommended
4. At least 1 Mb of hardware space available

1.6.2 Software Requirements

The software needed to support Cypercrypt are minimal , all the software a company needs to be installed are as follows:

1. A standard desktop operating system such as Windows 95/98/00/NT
2. A required system files and libraries that come with the specified operating system

University of Malaya

1.7 PROJECT SCHEDULE

All the activities needed to develop the project must be completed within a time constrain. This is vital and important for the project by following the schedule prepared, the final product can be achieved at or before the intended deadline.

The schedule is design based on the importance of workload of every activity in the project. The higher the importance of the workload, the more time the particular activity is given to complete it. After proper research and consideration, it is decided the most suitable and appropriate schedule to complete the project is as shown in Table 1.1

MONTH ACTIVITIES	JUN	JULY	AUG	SEPT	OCT	NOV	DEC	JAN	FEB
Resource searching and reading	■	■							
Literature review	■	■							
System analysis		■	■						
Proposal writing finalization	■	■	■						
System design					■	■	■		
Module Implementaton							■		
Coding & testing								■	■
System integration & testing					■	■	■	■	

Table 1.1 Project Schedule

University of Malaya

2.0 LITERATURE REVIEW

2.1 ANALYSIS OF EXISTING SYSTEMS

PGP stands for Pretty Good Privacy . It was inspired by Phil Zimmermann in the late of 80s. Zimmermann suggested using a cipher known as IDEA which is similar to DES. These scenario (email transmission between user A and user B) pictured how PGP actually works.

- To encrypt with IDEA, user A needs to choose a key but for user B to decrypt the message, user A somehow has to get the key to user B.

User A overcomes this problem by looking up user B's RSA public key and then uses it to encrypt the IDEA key. So, user A ends up sending two things to user B:

- It can securely delete files (called wiping), which overwrites files multiple times before erasing them so that no trace of the original file is still on user hard drive.
- If user make it a habit of signing your email before sending it, and then were infected with a virus that sends email to everyone in your address book, the recipients would know to discard your message and it's attachment if it were not signed by the user.

The disadvantages of PGP are:

- The majority of email users today do not use PGP, or any method of encryption, giving little opportunity for using it on a regular basis to stay familiar with it.
- Cryptography is a foreign concept for most people, and keeping up with keys, passphrases, and trust can be overwhelming for the casual user.
- Bad press relating to how encryption technology has been used in plotting terrorist attacks (a major point of contention, the debate of which is on-going).
- If the particular email software you use does not have a PGP plug-in available, it can be a challenge to use.

University of Malaya

2.2 SUGGESTED TOOLS

2.2.1 Suggested Programming Language:

1. Java
2. Visual Basic

These 2 programming languages are widely used in many applications .

Java was developed in the early nineties at Sun Microsystems as a platform-independent language. It incorporates many software engineering principles (object-oriented, strongly typed, good exception handling).Java basically used for writing applications that run on top of browsers.

Visual Basic allows programs to be built by pasting various pre-built components into a workspace. It is widely used for building database front-ends and prototypes that will be later written in other languages.

These are the lists of Java and Visual Basic advantages and disadvantages :

1. Java

Advantages of Java

•Portability / platform independent

•Object oriented

•Distributed / supports multithreading

•Secure

•Multimedia support

•Automated garbage collection

Disavantages of Java

•Significantly slower because it is interpreted, not compiled

•No templates (unlike C++) – "polymorphism"

University of Malaya

•Single, not multiple class inheritance

2. Visual Basic

Advantages of Visual Basic

•Easy to learn; similar to macro languages in Word, Excel, and MS Office

•Many add-ons

•Fast compiling

Disadvantages of Visual Basic

•Applications are large

•Applications require multiple large DLLs (dynamic link libraries) to run

•Writing really good graphical applications is difficult

•Windows API function calling is not good

2.2.2 Suggested encryption/decryption Module

1. Asymmetric encryption (Public/Private encryption)
2. Symmetric encryption (Secret Key or Shared Key)

1. Asymmetric encryption (Public/Private encryption)

Advantages of Assymetric Encryption

1. The private keys do not ever need to transmitted or revealed to anyone .So, it is more secure.
2. public-key systems can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. A sender can then r epudiate a previously signed message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret.

University of Malaya

Disadvantages of Assymetric Encryption

1. Low speed-there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method

2. Symmetric encryption (Secret Key or Shared Key)

The algorithms were all single key or conventional encryption algorithms, in which both the encrypt and the decrypt process use the same key, which must be kept secret.

Advantages of Symmetric Encryption

1. As long as the key remains secret, the systems also provides authentication, proof that a message received was not fabricated by someone other than the declared sender.
2. Speed- Secret-key is faster and can provide the same level of encryption strength as public-key systems do. For example, in a closed banking system, a single authority knows and manages all of the keys already so it makes sense to implement the faster of the two systems.
3. Secret key cryptography is the best system to use in a single person environment, such as encrypting your own personal files.

Disadvantages of Symmetric Encryption

1. With all key systems, if the key is revealed, the interceptors can immediately decrypt all encrypted information they have available. For this reason, in secure encryption systems, the keys are changed fairly frequently so that a compromised key will reveal only a limited amount of information.
2. Distribution of keys becomes a problem. Keys must be transmitted with utmost security because they allow access to all information encrypted under them.

University of Malaya

3.0 SYSTEM METHODOLOGIES

3.1 METHODOLOGIES

The main purpose of the development strategy is to evaluate the issues and characteristics of the proposed product, the decide wether it is feasible to develop the product. Analysing and determining the requirements of the products as well as the needs of the user is also part of the development strategy.

There are variety of development strategies appropriate for developing systems. The common models available are the Waterfall System, V Model, Spiral Model, Prototyping Model and the system development life cycle (SDLC). After careful evaluation it is decided that Ciphercrypt will be developed using the Prototyping Model due to its suitable features and structures.

Prototyping is a process that enables the development to create a model of the system that is going to be built. The Prototyping Model allows all part or part of the system to be constructed quickly to understand or clarify issues. In this model, the requirements and design of the system require repeated investigation to ensure that the developer and the user have a common understanding of what is needed and what is proposed.

The initial design can be revised until the developer and the user are happy with the performance of the system. Eventually the prototype system is coded and alternatives are considered with possible iterations, through requirements and design again. The prototype may not contains all the features or perform all the necessary functions of the final system but rather it includes sufficient elements for evaluation to be conducted. The main goal of the prototyping model is to reduce risk and uncertainty in development.

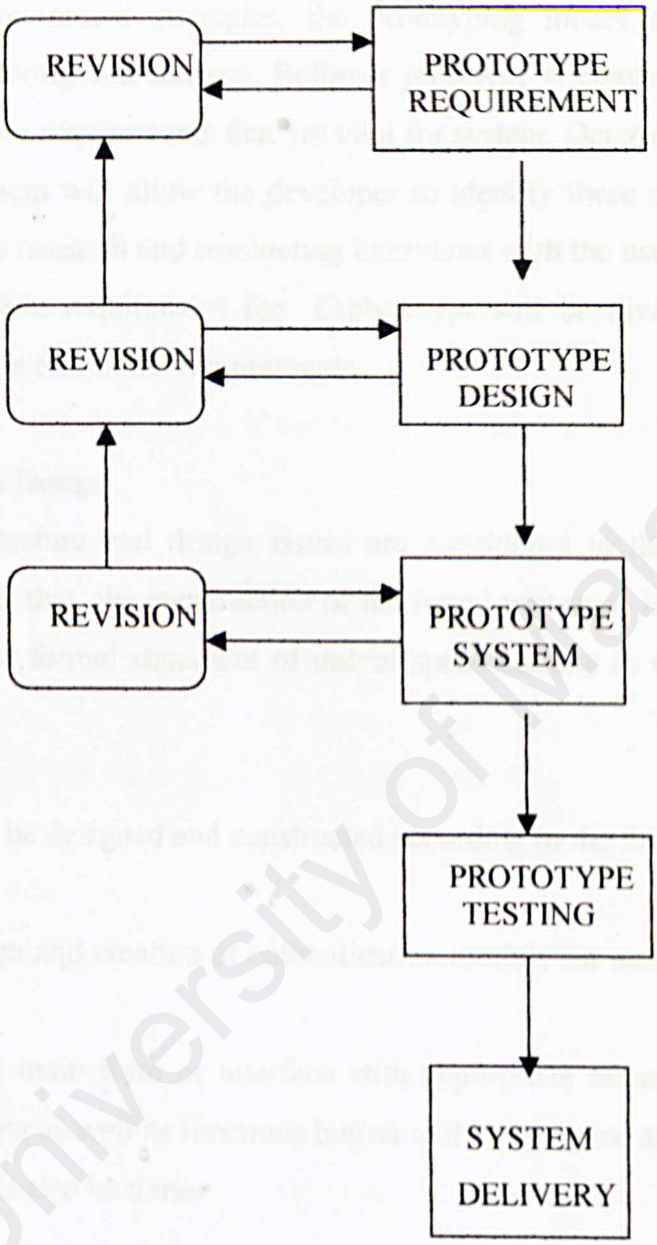


Figure 3.0 Prototyping Model

University of Malaya

1. Prototype Requirement

Alike other development strategies, the prototyping model approach too begin with requirement gathering and analysis. Before a prototype is constructed the developer must identify the known requirements that are vital for system. Determining the purpose and the scope of the system will allow the developer to identify these requirements. This can be achieved through research and conducting interviews with the users about their expectation of the system. The requirement for Ciphercrypt will be divided into two, which are functional and non functional requirements.

2. Prototype Design

Top level architecture and design issues are considered in the prototype design stage. Immediately after that, the construction of the initial prototype is done. During the period, documentation or formal statement of output specifications as well as software design is not done.

Ciphercrypt will be designed and constructed according to the following steps:

1. The design and creation of authentication module for user verification will be done first.
2. Next, the main form or interface with appropriate menu, toolbars, user input and output area as well as functions button will be designed and created. Other required forms will also be done.
3. The encryption and decryption module as well as other vital functionality for Ciphercrypt will be designed and coded.
4. Finally, the help module which includes the general information on Ciphercrypt, the user manual and etcetera will be designed.

University of Malaya

The Ciphercrypt prototype will be tested in all aspects based in its creation. Testing will be conducted by the developer as well as appointed testers to attain some valuable feedback regarding the system. Testing is performed to detect errors, inadequacies, limitations or drawback of the system.

1. Prototype System

Based on the information obtained during the testing stage, evaluation will be done on the prototype. All the faults of the system will be carefully evaluated and analyzed by the developer. The evaluation of the system will determine the features to be added on or excluded completely.

2. Revisions

The process may be repeated several times as needed to improve the system. The iteration process occurs until the system has evolved into a system with all the necessary features and characteristics that the developer is happy and satisfied with.

3. System Delivery

Once the features of the Ciphercrypt prototype is decided that it will meet the user needs and demands the system is finalized and implemented as a working system.

3.2 FINDINGS

Before developing a system, research must be done to acquire the information needed for the task. The information can be obtained from a variety of sources such as books, internet, magazines, journal as well as reports or projects done by other students. In order to obtain the information needed proper search methods must be employed.

University of Malaya

For my project I mainly used the internet due to the lack of reference books available on cryptography. However I managed to obtain a few books that were related from main library and friends. I also did attain some valuable information from lecture notes provided by my lecturer as well as previous reports and projects done by students. Using the proper keyword and terms allowed me to achieve the information needed. These are the terms that used to gather the information:

1. Cryptography, Encryption Algorithm Symmetric/Conventional System
2. Computer security and encryption, substitution cipher, block ciphers
3. RSA Encryption, DES Encryption

The following is a list of internet search engines:

1 www.yahoo.com
2 www.google.com
3 www.37.com
4 www.hotbot.com
5 www.altavista.com

3.3 SELECTED TOOLS

After doing further reading and searching through internet, I've decided to use Active Server Page (ASP) and Symmetric Key Encryption System to design and build the whole system. These are the advantages ASP and Symmetric Key Encryption Sytem that have been elaborated with more details in the Literature Review Chapter.

3.3.1 VB Advantages

University of Malaya

These are the main advantages of VB Programming Language:

- VB provides powerful features like a graphical user interface (GUI) and OD features by using more paint metaphor.
- VB can handles access to WIN 32.

- VB allows programmer to add user interface features like buttons by simply dragging and dropping controls provided.
- VB always being a chosen language to develop prototypes especially throw away prototype.

VB has access to be built in reusable component that finally will be incorporated into programs.

University of Malaya

3.3.2 Symmetric Key Encryption's Advantages

1. As long as the key remains secret, the systems also provides authentication, proof that a message received was not fabricated by someone other than the declared sender.

2. Speed- Secret-key is faster and can provide the same level of encryption strength as public-key systems do. For example, in a closed banking system, a single authority knows and manages all of the keys already so it makes sense to implement the faster of the two systems.

3. Secret key cryptography is the best system to use in a single person environment, such as encrypting your own personal files.

University of Malaya

3.4 FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

3.4.1 Functional Requirements

1. Authentication Module

   During this session, the user need to enter their username and password to enable them to proceed to the next screen.

2. Encryption/Decryption Module

   During this session, users don't need to waste their time on choosing a prime number to generate a secret key. The system will automatically encrypt the message after they click the 'send' button. The encrypted message will then be decrypted after the recipient click the 'open message' button.

3.4.2 Non-Functional Requirements

1. Maintainability

   The system should be easy to maintain. This means that users with the right access should be allowed to change the data inside the system, be it system data or information inside the key databases.

2. Robustness

   The system should be able to restart or continue after an error such as a system crash or a corrupted public key database.

3. Response Time

   The response time for any request should not be more twenty seconds.

University of Malaya

4. User-Friendliness

   The interface must have simple, easy to understand, self-explanatory buttons and forms. The graphical user interface must look very simple compared to the existing encryption product. This must take into account especially to attract the new, inexperienced users such as students and also small companies.

5. Flexibility

   The user can either decrypt the message and keep it first and send it later or send it right after the encryption process.

University of Malaya

4.0 SYSTEM DESIGN

4.1 System Flowchart

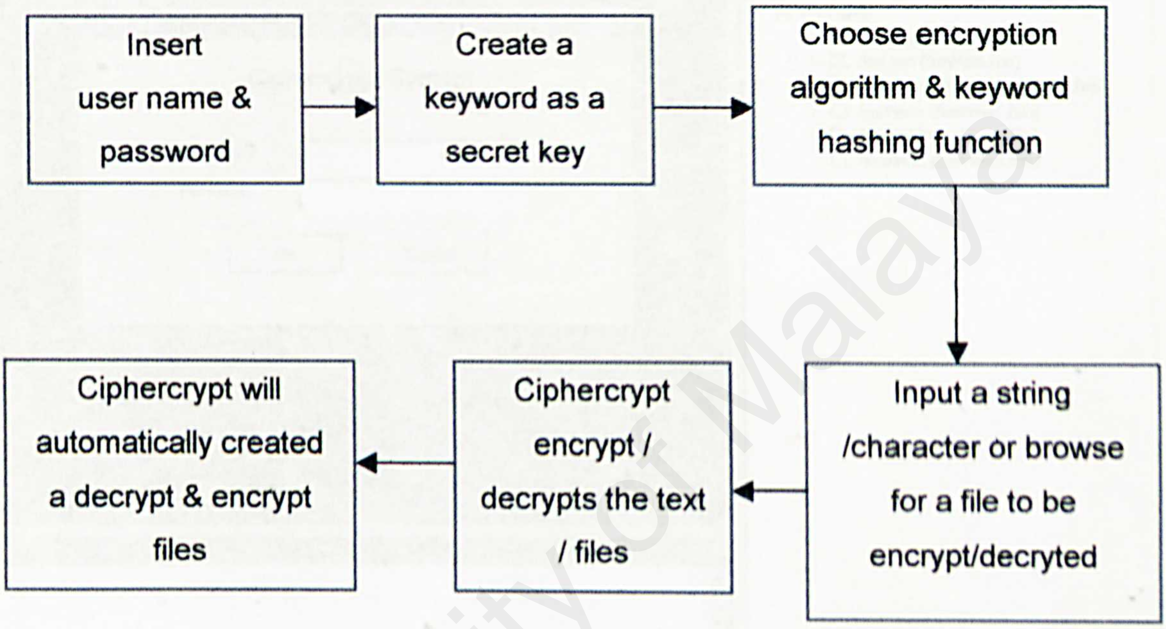

Insert user name & password
Create a keyword as a secret key
Choose encryption algorithm & keyword hashing function
Input a string /character or browse for a file to be encrypt/decryted
Ciphercrypt encrypt / decrypts the text / files
Ciphercrypt will automatically created a decrypt & encrypt files

Figure 4.1: Flowchart of The Ciphercrypt System

University of Malaya

4.2 SYSTEM INTERFACE

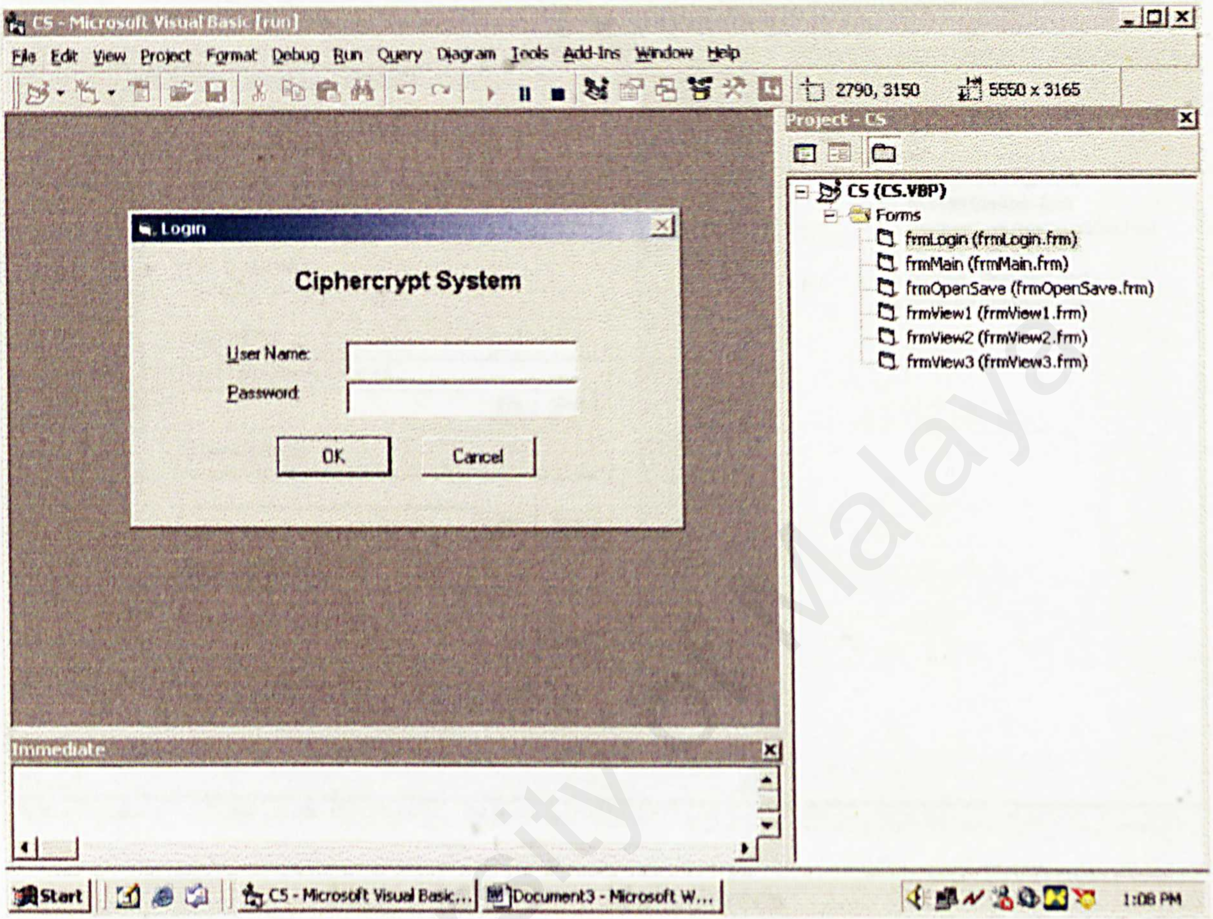
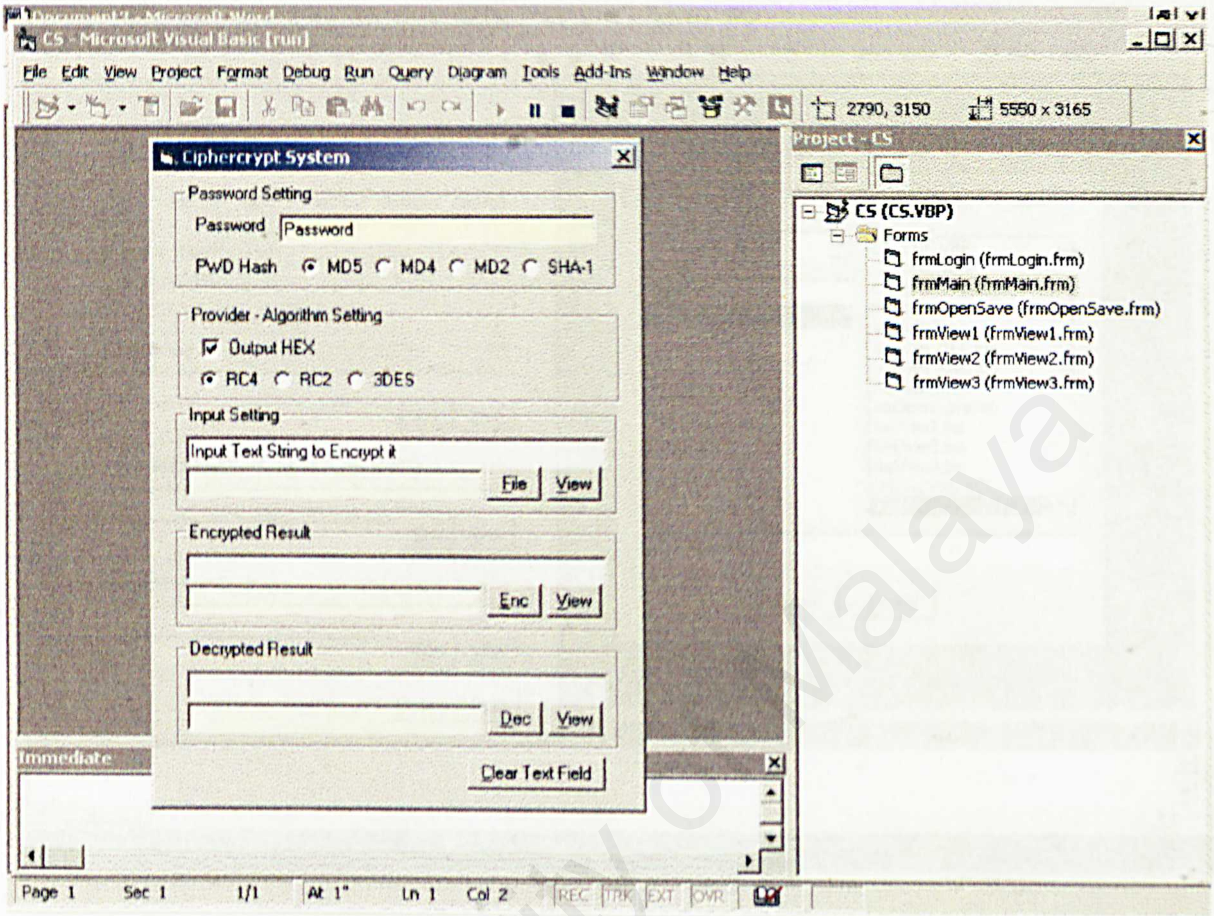


Figure 4.2.1 Authentication Screen

University of Malaya


Document2 - Microsoft Word
CS - Microsoft Visual Basic [run]
File Edit View Project Format Debug Run Query Diagram Tools Add-Ins Window Help
2790, 3150
5550 x 3165
Project - CS
CS (CS.VBP)
Forms
frmLogin (frmLogin.frm)
frmMain (frmMain.frm)
frmOpenSave (frmOpenSave.frm)
frmView1 (frmView1.frm)
frmView2 (frmView2.frm)
frmView3 (frmView3.frm)
Immediate
Page 1 Sec 1 1/1 At 1" Ln 1 Col 2 REC TRK EXT OVR

Ciphercrypt System

Password Setting

Password: Password

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

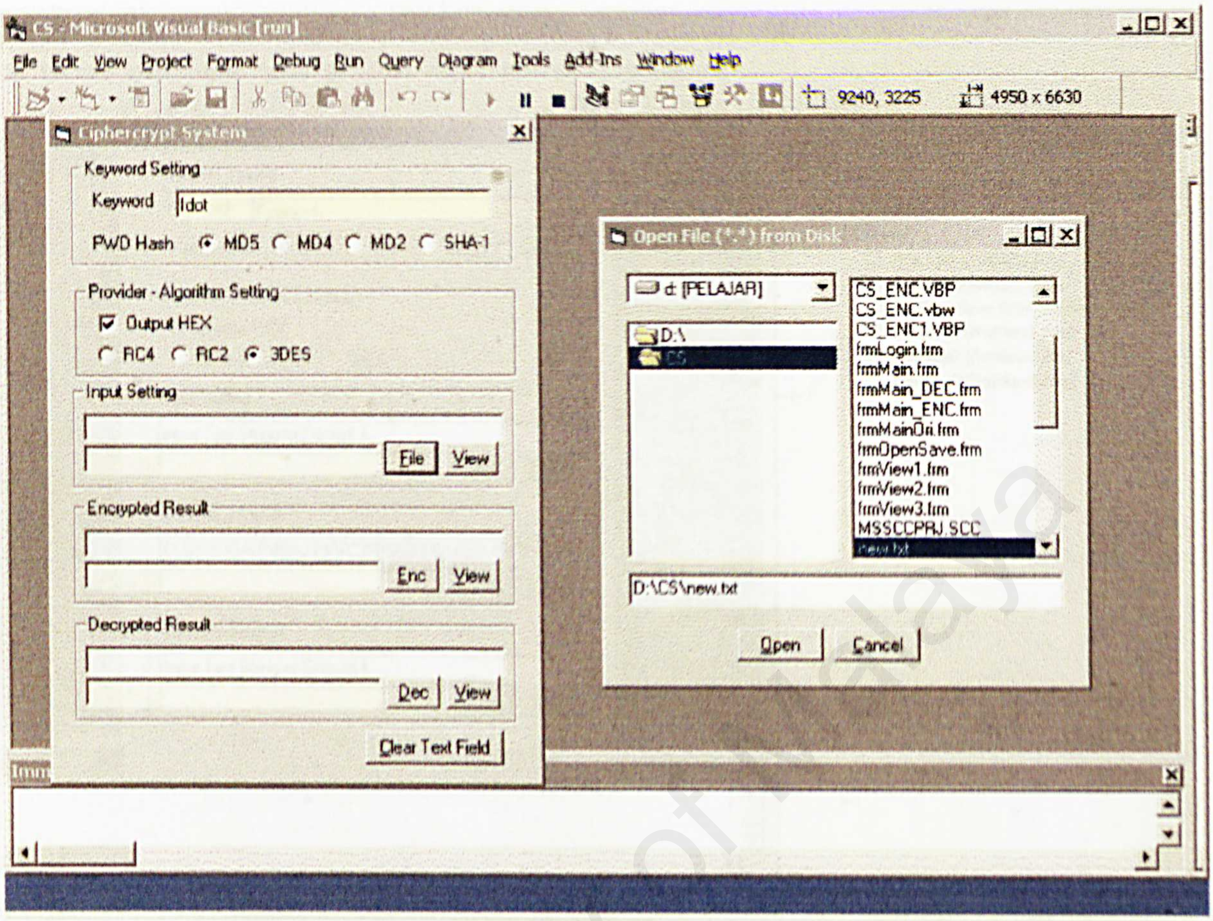
● RC4 ○ RC2 ○ 3DES

Input Setting

Input Text String to Encrypt it

Figure 4.2.2 Main Screen

University of Malaya



CS - Microsoft Visual Basic [run]
File Edit View Project Format Debug Run Query Diagram Tools Add-Ins Window Help
9240, 3225
4950 x 6630
Ciphercrypt System
Open File (*.*) from Disk
File
View
Enc
View
Dec
View
Clear Text Field
Open
Cancel
Imm

Keyword Setting

Keyword: Idot

PWD Hash: ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

○ RC4 ○ RC2 ● 3DES

Input Setting

Encrypted Result

Decrypted Result

d: [PELAJAR]

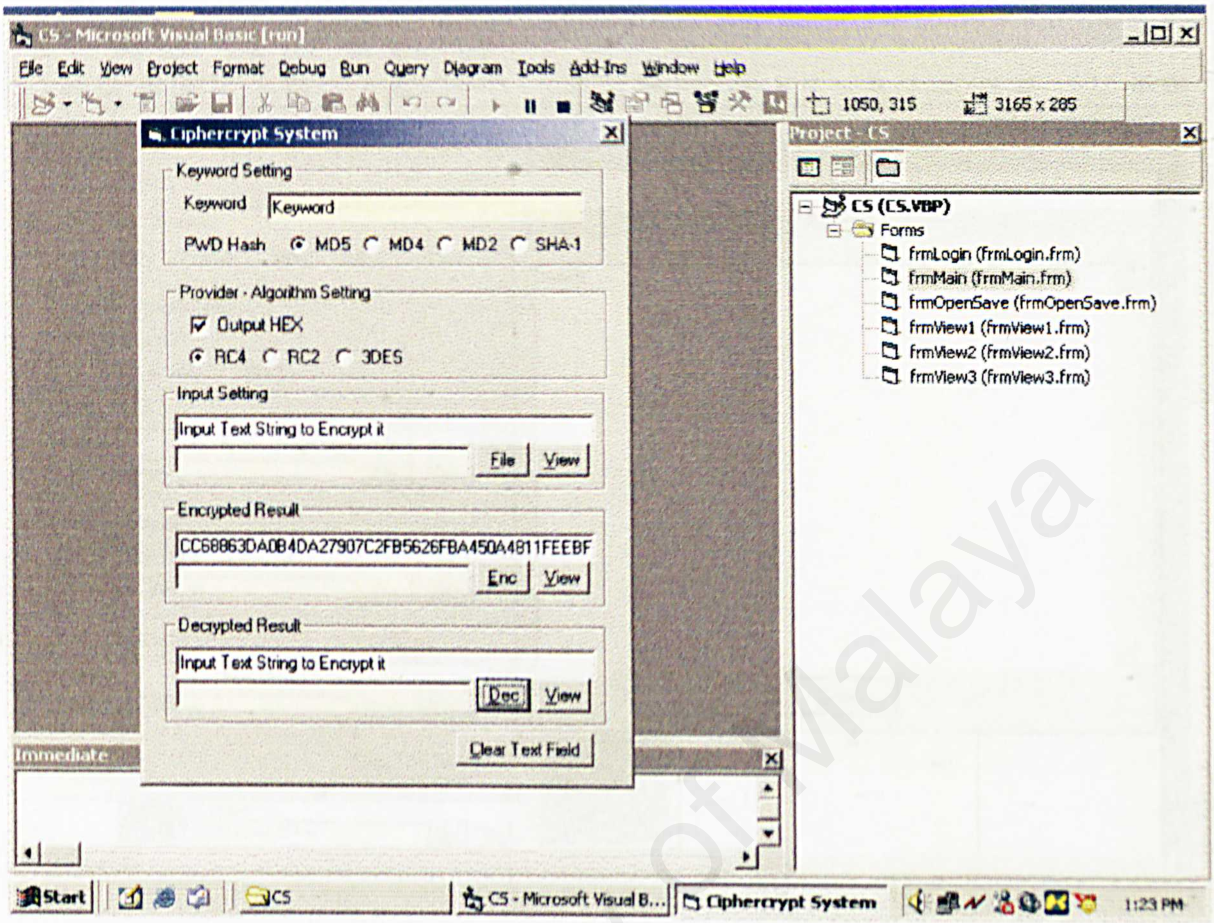
D:\
CS

CS_ENC.VBP
CS_ENC.vbw
CS_ENC1.VBP
frmLogin.frm
frmMain.frm
frmMain_DEC.frm
frmMain_ENC.frm
frmMainOri.frm
frmOpenSave.frm
frmView1.frm
frmView2.frm
frmView3.frm
MSSCCPRJ.SCC
new.txt

D:\CS\new.txt

Figure 4.2.3 Open File Screen

University of Malaya



Ciphercrypt System

Keyword Setting

Keyword: Keyword

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

Input Text String to Encrypt it

Encrypted Result

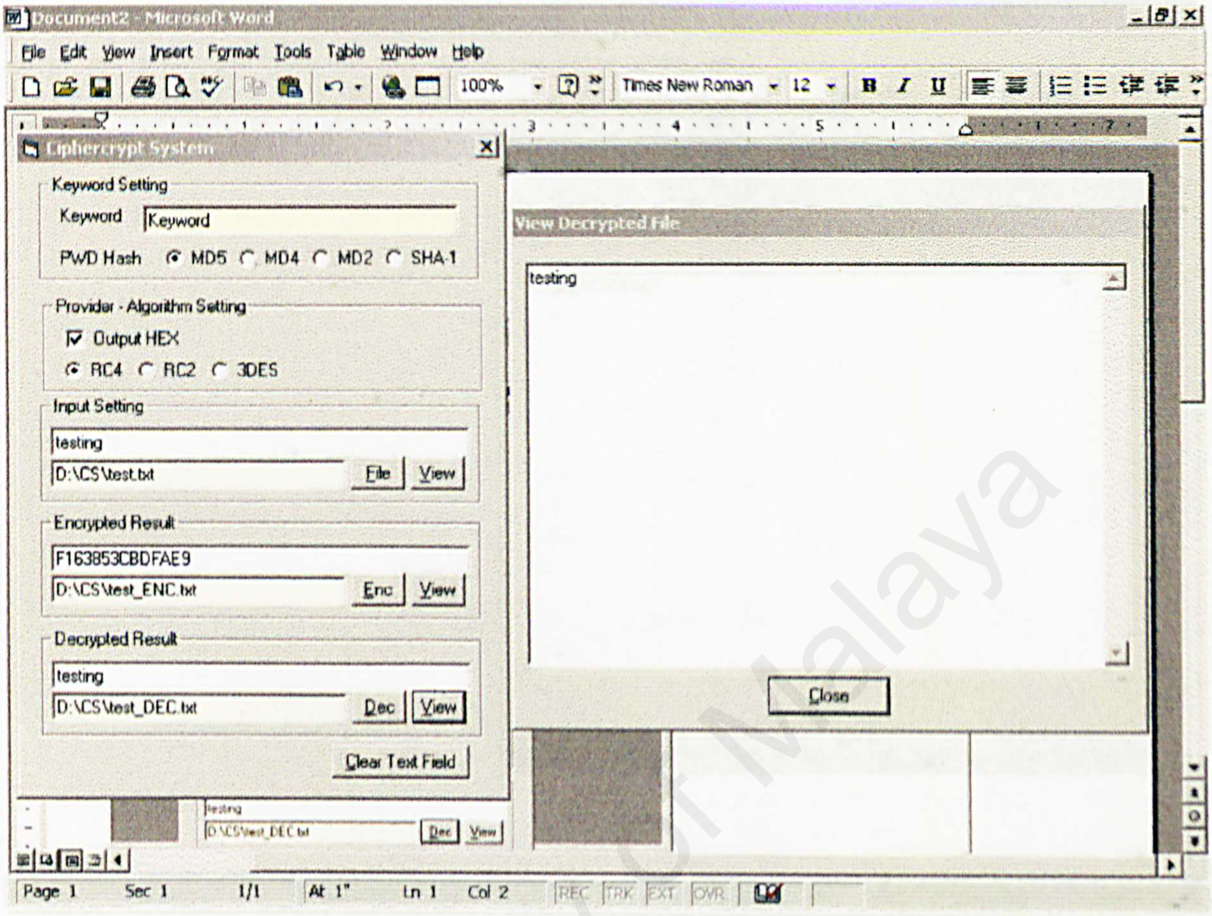
CC68863DA0B4DA27907C2FB5626FBA450A4811FEEBF

Decrypted Result

Input Text String to Encrypt it

Figure 4.2.4 String (Encrytion / Decryption)

University of Malaya



Document2 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
100%
Times New Roman
12
Ciphercrypt System
View Decrypted File
File
View
Enc
View
Dec
View
Clear Text Field
Close
Page 1 Sec 1 1/1 At 1" Ln 1 Col 2 REC TRK EXT OVR

Keyword Setting

Keyword: Keyword

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

testing

D:\CS\test.txt

Encrypted Result

F163853CBDFAE9

D:\CS\test_ENC.txt

Decrypted Result

testing

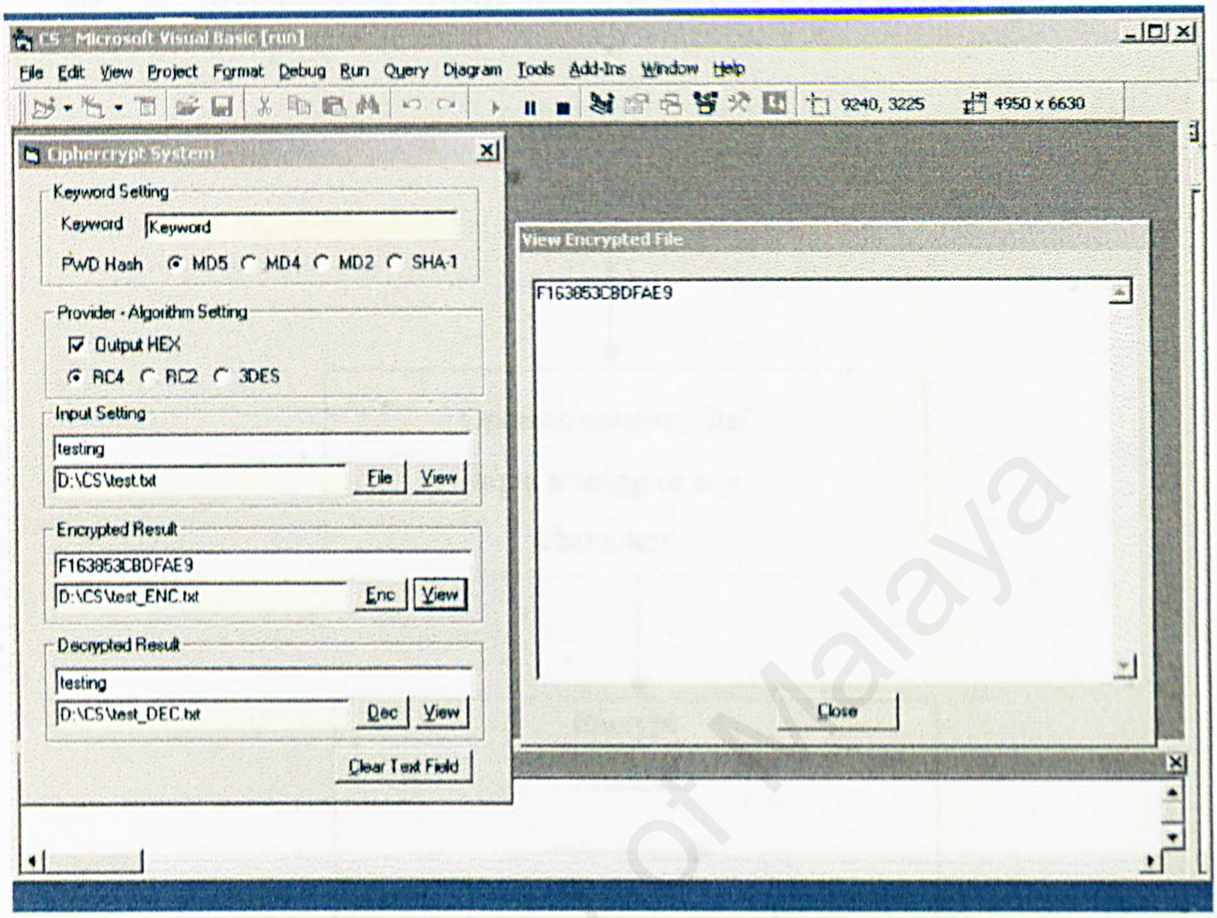
D:\CS\test_DEC.txt

View Decrypted File

testing

Figure 4.2.5 View Screen (Decrypted Output)

University of Malaya



CS - Microsoft Visual Basic [run]
File Edit View Project Format Debug Run Query Diagram Tools Add-Ins Window Help
9240, 3225
4950 x 6630
Ciphercrypt System

Keyword Setting

Keyword: Keyword

PWD Hash: ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

testing

D:\CS\test.txt

Encrypted Result

F163853CBDFAE9

D:\CS\test_ENC.txt

Decrypted Result

testing

D:\CS\test_DEC.txt

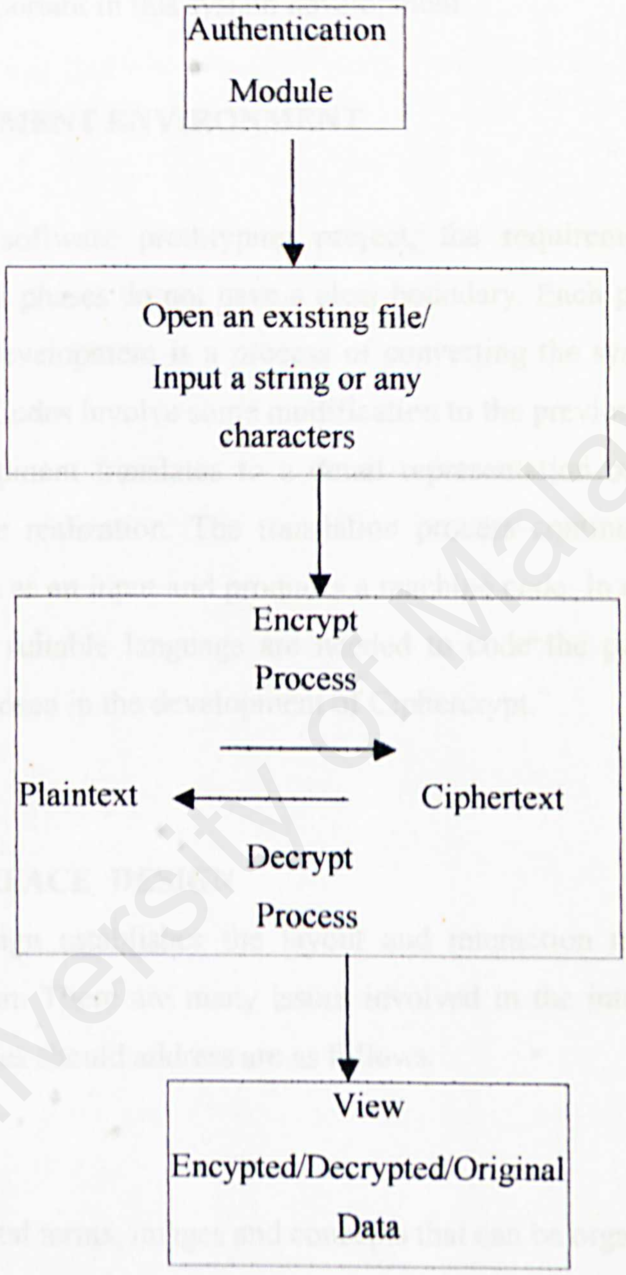
File
View
Enc
View
Dec
View
Clear Text Field
View Encrypted File

F163853CBDFAE9

Figure 4.2.6 View Screen (Encrypted Output)

University of Malaya

5.0 SYSTEM DEVELOPMENT & IMPLEMENTATION



University of Malaya

5.1 INTRODUCTION

System implementation is the construction of the new system and the delivery of that system into production. It involves the translation of the software representation produce by the design phase into a computer readable form. This phase at any time involves some modifications to the previous design.

This section states and discusses all the software and hardware tools used in thedevelopment of Ciphercrypt. The decision of choosing and using suitable programming tools was also very important in this system development.

5.2 DEVELOPMENT ENVIRONMENT

Usually in a software prototyping project, the requirement analysis, system designand development phases do not have a clear boundary. Each phase tends to involve one another. System development is a process of converting the system requirement and designs into program. Codes involve some modification to the previous design.

System development translates to a detail representation of the software into a programming language realization. The translation process continues when a computer accepts a source codes as an input and produces a machine code. In order to carry that out, appropriate tools and suitable language are needed to code the program. A number of software tools were chosen in the development of Ciphercrypt.

University of Malaya

5.3 INTERFACE DESIGN

The interface design establishes the layout and interaction mechanism for human machine interaction. There are many issues involved in the interface design, the key issues that interfaces should address are as follows:

1. Metaphor

   The fundamental terms, images and concepts that can be organized and learned.
2. A Mental Modes

   The organization and representation of data, functions, task and roles.
3. The Navigation Rules For The Model

   How to move among data, functions, activities and roles.
4. Look

   The character of the system's appearance that convey information to the user.

5.4 HARDWARE TOOLS

1. Personal Computer

The personal computer that was used to develop Ciphercrypt has the following capabilities or specifications

- AMDK6 450MHz microprocessor
- 32Mb SDRAM
- 10Gb hard disk
- 44X Max CD-ROM drive
- Standard 3 ½ inch floppy
- 14 " monitor and other standard peripheral

2. Other different hardware hardware that was utilized in the development of Ciphercrypt is a printer , scanner photocopier for various purpose

5.5 SOFTWARE TOOLS

1. Microsoft Windows 98

Microsoft Windows 98 was the desktop operating system used for the development of Ciphercrypt. This is because Windows 98 supports a vast array of software and development tools. Windows 98 provides a multitasking environment, scalability, portability and also reliable.

2. Windows Notepad

Windows Notepad is used during the viewing process of encrypt/decrypted output.

3. Visual Basic Language (VB)

The main programming tool used for developing Ciphercrypt was Visual Basic (VB). This software selected because of the following reasons:

University of Malaya

- VB provides powerful features like a graphical user interface (GUI) and OD features by using more paint metaphor.
- VB can handles access to WIN 32.
- VB allows programmer to add user interface features like buttons by simply dragging and dropping controls provided.
- VB always being a chosen language to develop prototypes especially throw away prototype.
- VB has access to be built in reusable component that finally will be incorporated into programs.

5.6 DEVELOPMENT OF CIPHERCRYPT

In this part, the development of all forms on screens are shown and briefly described. The vital and major codes involved are also shown in this section

4.6.1 Screen Development

Ciphercrypt only has a few screens with simple interfaces. This is very suitable for the used of the first time user. These screens were developed using the Microsoft Frontpage. It provides a very flexible and user friendly form editor, hence making the development of the screens much easier as well as faster.

The screens that exist in Ciphercrypt are namely Login Screen, Main Screen and Open File Screen, Encrypt/Decrypt Output File Screen and View Screen. The following are the screen shown in chronological order, from the start of Ciphercrypt until the user exit the application.

University of Malaya

1. Main Screen

Main screen is the most important of Ciphercrypt. The user will only be able to see this screen if the username and password are verified to be legitimated by the system. In the main screen, the user is able to perform all the functions available in Ciphercrypt. This screen is provided with many buttons with their own function. The File Button is use to open an existing file, Encrypt/Decrypt button to encrypt/decrypt files or any string characters, View button to view either original text, decrypted text (plaintext), or encrypted text (ciphertext) separately and also Clear All Text button to clear the screen.

2. Authentication Screen

This screen will require the users to enter a user name and password before proceeding to the main screen. To proceed, both the required details must be correct. All the other screen are accessible from Authentication Screen.

The purpose of this Authentication Screen is to maintain the integrity of Ciphercrypt and to prevent an unauthorized user to use the program . As we know, integrity is a vital aspect in encryption system.

5.6.2 Codes Development

Coding performs task which translate a design into a machine-readable form. If the design is created in detailed manner, the code generation can be accomplished with much ease. Therefore, codes are the core and backbone of every application. The codes are what that makes the various function in an application possible. The codes for Ciphercrypt are all written using Visual Basic Programming Language (VB).

Visual basic is a Microsoft Window's Programming Language. It's programs are created in an Integrated Development Environment which allows programmers to debug and run VB easily. VB is also known as a Rapid Application Development Language because of it's ability to develop a system in a short period. VB is

University of Malaya

derived from the BASIC language but it varies from Basic since VB can provides more powerful user interface by using more paint metaphor.

All the screens that make up Ciphercrypt consist of codes are now functions and behave in the manner expected. All the important codes will be shown except for actual encryption and decryption module for security.

By practicing good programming methods, it will be easy to produce a reliable and maintainable application. A good programming or coding methods always requires features such as readability of the code, good naming techniques for the variable controls and modules and internal documents for better understanding.

5.6.2.1 Login Screen Coding

```
Option Explicit
        Private Declare Function DeleteMenu Lib "user32"
            (ByVal hMenu As Long, ByVal nPosition As Long, ByVal wFlags As
            Long) As Long
          Private Declare Function GetSystemMenu Lib "user32"
          (ByVal hWnd As Long, ByVal bRevert As Long) As Long
        Private Const MF_BYPOSITION = &H400&
        Public LoginSucceeded As Boolean

        'Function to remove the windows close button ('x')
        Private Sub RemoveMenus()
          Dim hMenu As Long
          hMenu = GetSystemMenu(hWnd, False)
          DeleteMenu hMenu, 6, MF_BYPOSITION
        End Sub
```

University of Malaya

```
Private Sub Form_Load()
RemoveMenus
End Sub

'If cancel button is pressed quit HIS
Private Sub cmdCancel_Click()
   LoginSucceeded = False
   Dim out
   out = MsgBox("Are you sure you want to quit this program?", vbYesNo, "HIS")
   If out = vbYes Then
   End
   ElseIf out = vbNo Then
   txtUserName.SetFocus
   Exit Sub
   End If
 End Sub

 'Check for correct password and username
 Private Sub cmdOK_Click()
    If txtPassword = "password" And txtUserName = "CS" Then
       LoginSucceeded = True
       frmMain.Show
       Unload Me
    Else
       If txtUserName = "CS" Then
```

University of Malaya

```
          MsgBox "Incorrect password, please enter the correct password", , "HIS"
          txtUserName.SetFocus
          Else

     MsgBox "Incorrect username, please enter the correct username", , "CS"
          txtPassword.SetFocus
          SendKeys "{Home}+{End}"
          End If
       End If
     End Sub
```

5.6.2.2 Main Screen Code

```
Option Explicit

Private EnDecrypt As New CryptoDLL.FileString


Private Sub Command1_Click()
If txtFile.Text = "" Then frmView1.Text1.Text = txtString.Text
frmView1.Show

End Sub


Private Sub Command2_Click()
If txtEncFile.Text = "" Then frmView2.Text1.Text = txtEncString.Text
frmView2.Show
```

University of Malaya

```
End Sub

Private Sub Command3_Click()
If txtDecFile.Text = "" Then frmView3.Text1.Text = txtDecString.Text
frmView3.Show
End Sub

Private Sub Command4_Click()
txtString.Text = ""
txtEncString.Text = ""
txtDecString.Text = ""
txtFile.Text = ""
txtEncFile.Text = ""
txtDecFile.Text = ""

End Sub

Private Sub Form_Load()
  With Me
    .Move (Screen.Width - .Width) \ 2, (Screen.Height - .Height) \ 2
  End With


End Sub
```

University of Malaya

```
Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As Integer)
 Set EnDecrypt = Nothing
End Sub

Private Sub Form_Unload(Cancel As Integer)
 End
End Sub

Private Sub cmdEnc_Click()
 Dim blnRetVal As Boolean

 With EnDecrypt
  .Password = Trim$(txtPWD.Text)
  '.Provider = CBool(chkEnhanced.Value)
  .ConvertHEX = CBool(chkHEX.Value)
  .HashType = HashType
  .CipherType = CipherType
```

University of Malaya

5.6.2.3 Encryption Code

```
'Encrypt String
   If Trim$(txtString.Text) <> "" Then
     txtEncString.Text = .EncryptString(Trim$(txtString.Text), blnRetVal)
     frmView2.Text1.Text = txtEncString.Text
'Return True if success
'Debug.Print blnRetVal
   End If

'Encrypt File
   If Trim$(txtFile.Text) <> "" Then
     blnRetVal = .EncryptFile(Trim$(txtFile.Text), Trim$(txtEncFile.Text))
'Return True if success

'frmView2.Text1.Text = blnRetVal
'Debug.Print blnRetVal
   End If
  End With
End Sub

Private Sub cmdDec_Click()
  Dim blnRetVal As Boolean

  With EnDecrypt
```

University of Malaya

```
  .Password = Trim$(txtPWD.Text)
  '.Provider = CBool(chkEnhanced.Value)
  .ConvertHEX = CBool(chkHEX.Value)
  .HashType = HashType
  .CipherType = CipherType
```

5.6.2.4 Decryption Code

```
'Decrypt String
  If Trim$(txtEncString.Text) <> "" Then
   txtDecString.Text = .DecryptString(Trim$(txtEncString.Text), blnRetVal)


 frmView3.Text1.Text = txtDecString.Text
'Return True if success
'Debug.Print blnRetVal
  End If

'Decrypt File
  If Trim$(txtEncFile.Text) <> "" Then
   blnRetVal = .DecryptFile(Trim$(txtEncFile.Text), Trim$(txtDecFile.Text))
'Return True if success
'frmView3.Text1.Text = blnRetVal
'Debug.Print blnRetVal
  End If
 End With
End Sub
```

University of Malaya

```
Private Function HashType() As Integer
 Dim i As Integer
 For i = 0 To 3
  If optHash(i).Value Then
   HashType = i + 1
   Exit For
  End If
 Next
End Function

Private Function CipherType() As Integer
 Dim i As Integer
 For i = 0 To 4
  If optCipher(i).Value Then
   CipherType = i + 1
   Exit For
  End If
 Next
End Function

Private Sub cmdFile_Click()
Dim temp$
```

University of Malaya

```
Dim alltext$

On Error Resume Next
 Dim strFilePath As String
 Dim intFileEx As Integer

 strFilePath = OpenSaveFile(1, "*.*")
 If strFilePath = "" Then Exit Sub
 txtFile.Text = strFilePath


 Open strFilePath For Input As #1
  While Not EOF(1)
  Line Input #1, temp$
  alltext$ = alltext$ & temp$ & vbCrLf
  Wend
  txtString.Text = alltext$
  frmView1.Text1.Text = alltext$
 Close #1


 intFileEx = InStrRev(strFilePath, ".")
 txtEncFile.Text = Left$(strFilePath, intFileEx - 1) & "_ENC" & Mid$(strFilePath,
intFileEx)


 txtDecFile.Text = Left$(strFilePath, intFileEx - 1) & "_DEC" & Mid$(strFilePath,
intFileEx)
```

University of Malaya

```
End Sub


Private Function OpenSaveFile(Optional intFlag As Integer = 1, Optional strPattern As String = "*.*") As String
'Return selected File Path + Name; Return "" if no File selected
'intFlag = 0: Save; intFlag = 1: Open
'strPattern = File Extensions, separated by ";", no Space !!!
 Dim strTemp As String

 frmOpenSave.InitForm intFlag, strPattern
 strTemp = Trim$(frmOpenSave.Text1.Text)
 Unload frmOpenSave
'not a File, but Folder
 If Right$(strTemp, 1) = "\" Then strTemp = ""

 OpenSaveFile = strTemp
End Function
```

5.6.2.5 Open File Screen Code

```
Option Explicit

Private EnDecrypt As New CryptoDLL.FileString


Private Sub Command1_Click()
```

University of Malaya

```
If txtFile.Text = "" Then frmView1.Text1.Text = txtString.Text

frmView1.Show

End Sub


Private Sub Command2_Click()

If txtEncFile.Text = "" Then frmView2.Text1.Text = txtEncString.Text

frmView2.Show

End Sub


Private Sub Command3_Click()

If txtDecFile.Text = "" Then frmView3.Text1.Text = txtDecString.Text

frmView3.Show

End Sub


Private Sub Command4_Click()

txtString.Text = ""

txtEncString.Text = ""

txtDecString.Text = ""

txtFile.Text = ""

txtEncFile.Text = ""

txtDecFile.Text = ""

End Sub


Private Sub Form_Load()
```

University of Malaya

```
 With Me

.Move (Screen.Width - .Width) \ 2, (Screen.Height - .Height) \ 2
 End With

End Sub

Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As Integer)
 Set EnDecrypt = Nothing
End Sub

Private Sub Form_Unload(Cancel As Integer)
 End
End Sub

Private Sub cmdEnc_Click()
 Dim blnRetVal As Boolean

 With EnDecrypt

 .Password = Trim$(txtPWD.Text)
  '.Provider = CBool(chkEnhanced.Value)
  .ConvertHEX = CBool(chkHEX.Value)
  .HashType = HashType
```

University of Malaya

```
  .CipherType = CipherType

'Encrypt String
  If Trim$(txtString.Text) <> "" Then
   txtEncString.Text = .EncryptString(Trim$(txtString.Text), blnRetVal)
   frmView2.Text1.Text = txtEncString.Text
'Return True if success
'Debug.Print blnRetVal
  End If

'Encrypt File
  If Trim$(txtFile.Text) <> "" Then
   blnRetVal = .EncryptFile(Trim$(txtFile.Text), Trim$(txtEncFile.Text))
'Return True if success
'frmView2.Text1.Text = blnRetVal
'Debug.Print blnRetVal
  End If
 End With
End Sub

Private Sub cmdDec_Click()
 Dim blnRetVal As Boolean

  With EnDecrypt
   .Password = Trim$(txtPWD.Text)
   '.Provider = CBool(chkEnhanced.Value)
```

University of Malaya

```
    .ConvertHEX = CBool(chkHEX.Value)

    .HashType = HashType

    .CipherType = CipherType


'Decrypt String

    If Trim$(txtEncString.Text) <> "" Then

     txtDecString.Text = .DecryptString(Trim$(txtEncString.Text), blnRetVal)

     frmView3.Text1.Text = txtDecString.Text

'Return True if success


'Debug.Print blnRetVal

   End If


'Decrypt File

    If Trim$(txtEncFile.Text) <> "" Then

     blnRetVal = .DecryptFile(Trim$(txtEncFile.Text), Trim$(txtDecFile.Text))

'Return True if success

'frmView3.Text1.Text = blnRetVal

'Debug.Print blnRetVal

    End If

  End With

 End Sub


 Private Function HashType() As Integer

  Dim i As Integer
```

University of Malaya

```
 For i = 0 To 3
  If optHash(i).Value Then
    HashType = i + 1
  Exit For
   End If
 Next
End Function

Private Function CipherType() As Integer
 Dim i As Integer
 For i = 0 To 4
  If optCipher(i).Value Then
    CipherType = i + 1
    Exit For
  End If
 Next
End Function


Private Sub cmdFile_Click()
Dim temp$
Dim alltext$

On Error Resume Next
 Dim strFilePath As String
```

University of Malaya

```
Dim intFileEx As Integer


strFilePath = OpenSaveFile(1, "*.*")

If strFilePath = "" Then Exit Sub

txtFile.Text = strFilePath


Open strFilePath For Input As #1

  While Not EOF(1)

  Line Input #1, temp$

  alltext$ = alltext$ & temp$ & vbCrLf

  Wend

  txtString.Text = alltext$

  frmView1.Text1.Text = alltext$

Close #1


intFileEx = InStrRev(strFilePath, ".")


txtEncFile.Text = Left$(strFilePath, intFileEx - 1) & "_ENC" & Mid$(strFilePath, intFileEx)


txtDecFile.Text = Left$(strFilePath, intFileEx - 1) & "_DEC" & Mid$(strFilePath, intFileEx)


End Sub
```

University of Malaya

```
Private Function OpenSaveFile(Optional intFlag As Integer = 1, Optional strPattern As
String = "*.*") As String
'Return selected File Path + Name; Return "" if no File selected
'intFlag = 0: Save; intFlag = 1: Open
'strPattern = File Extensions, separated by ";", no Space !!!
  Dim strTemp As String

  frmOpenSave.InitForm intFlag, strPattern
  strTemp = Trim$(frmOpenSave.Text1.Text)
  Unload frmOpenSave
'not a File, but Folder
  If Right$(strTemp, 1) = "\" Then strTemp = ""

  OpenSaveFile = strTemp
End Function
```

5.6.2.6 View Screen Code

```
Option Explicit

Private EnDecrypt As New CryptoDLL.FileString


Private Sub Command1_Click()
If txtFile.Text = "" Then frmView1.Text1.Text = txtString.Text
frmView1.Show
```

University of Malaya

```
End Sub

Private Sub Command2_Click()
If txtEncFile.Text = "" Then frmView2.Text1.Text = txtEncString.Text

frmView2.Show
End Sub

Private Sub Command3_Click()
If txtDecFile.Text = "" Then frmView3.Text1.Text = txtDecString.Text
frmView3.Show
End Sub

Private Sub Command4_Click()
txtString.Text = ""
txtEncString.Text = ""
txtDecString.Text = ""
txtFile.Text = ""
txtEncFile.Text = ""
txtDecFile.Text = ""

End Sub

Private Sub Form_Load()
```

University of Malaya

```
 With Me

  .

Move (Screen.Width - .Width) \ 2, (Screen.Height - .Height) \ 2

 End With


End Sub


Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As Integer)

 Set EnDecrypt = Nothing

End Sub


Private Sub Form_Unload(Cancel As Integer)

 End

End Sub


Private Sub cmdEnc_Click()

 Dim blnRetVal As Boolean


 With EnDecrypt

   .Password = Trim$(txtPWD.Text)

   '.Provider = CBool(chkEnhanced.Value)

   .ConvertHEX = CBool(chkHEX.Value)

   .HashType = HashType

   .CipherType = CipherType
```

University of Malaya

```
'Encrypt String
   If Trim$(txtString.Text) <> "" Then
     txtEncString.Text = .EncryptString(Trim$(txtString.Text), blnRetVal)
     frmView2.Text1.Text = txtEncString.Text
'Return True if success
'Debug.Print blnRetVal
   End If

'Encrypt File
   If Trim$(txtFile.Text) <> "" Then
     blnRetVal = .EncryptFile(Trim$(txtFile.Text), Trim$(txtEncFile.Text))
'Return True if success

'frmView2.Text1.Text = blnRetVal
'Debug.Print blnRetVal
   End If
 End With
End Sub

Private Sub cmdDec_Click()
 Dim blnRetVal As Boolean

  With EnDecrypt
   .Password = Trim$(txtPWD.Text)
   '.Provider = CBool(chkEnhanced.Value)
   .ConvertHEX = CBool(chkHEX.Value)
```

University of Malaya

```
   .HashType = HashType
   .CipherType = CipherType

'Decrypt String
   If Trim$(txtEncString.Text) <> "" Then

  txtDecString.Text = .DecryptString(Trim$(txtEncString.Text), blnRetVal)
    frmView3.Text1.Text = txtDecString.Text
'Return True if success
'Debug.Print blnRetVal
   End If

'Decrypt File
   If Trim$(txtEncFile.Text) <> "" Then
    blnRetVal = .DecryptFile(Trim$(txtEncFile.Text), Trim$(txtDecFile.Text))
'Return True if success
'frmView3.Text1.Text = blnRetVal
'Debug.Print blnRetVal
   End If
  End With
End Sub



Private Function HashType() As Integer
  Dim i As Integer
```

University of Malaya

```
 For i = 0 To 3
   If optHash(i).Value Then
     HashType = i + 1
     Exit For
   End If
 Next
End Function

Private Function CipherType() As Integer
  Dim i As Integer
  For i = 0 To 4
    If optCipher(i).Value Then
     CipherType = i + 1
     Exit For
    End If
  Next
End Function

Private Sub cmdFile_Click()
Dim temp$
Dim alltext$


On Error Resume Next
  Dim strFilePath As String
  Dim intFileEx As Integer
```

University of Malaya

```
  strFilePath = OpenSaveFile(1, "*.*")
  If strFilePath = "" Then Exit Sub
  txtFile.Text = strFilePath

  Open strFilePath For Input As #1
   While Not EOF(1)
   Line Input #1, temp$
   alltext$ = alltext$ & temp$ & vbCrLf
   Wend
   txtString.Text = alltext$

   frmView1.Text1.Text = alltext$
  Close #1

  intFileEx = InStrRev(strFilePath, ".")
  txtEncFile.Text = Left$(strFilePath, intFileEx - 1) & "_ENC" & Mid$(strFilePath,
intFileEx)

  txtDecFile.Text = Left$(strFilePath, intFileEx - 1) & "_DEC" & Mid$(strFilePath,
intFileEx)

End Sub
```

University of Malaya

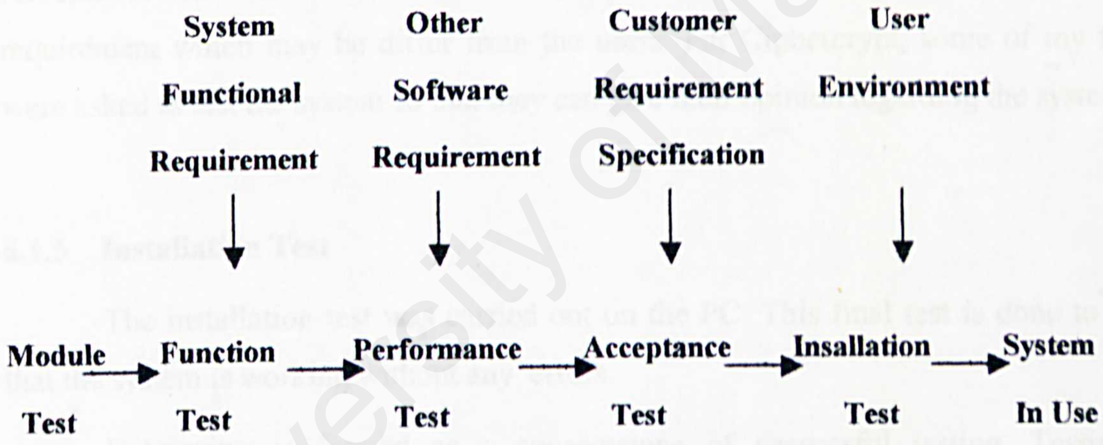
```
        Private Function OpenSaveFile(Optional intFlag As Integer = 1, Optional strPattern
        As String = "*.*") As String
        'Return selected File Path + Name; Return "" if no File selected
        'intFlag = 0: Save; intFlag = 1: Open
        'strPattern = File Extensions, separated by ";", no Space !!!
          Dim strTemp As String


          frmOpenSave.InitForm intFlag, strPattern
          strTemp = Trim$(frmOpenSave.Text1.Text)
          Unload frmOpenSave
        'not a File, but Folder
          If Right$(strTemp, 1) = "\" Then strTemp = ""

          OpenSaveFile = strTemp
End Function
```

University of Malaya

6.0 SYSTEM TESTING

Testing is a vital and critical element for the assurance of the program quality. It also represent the ultimate review of the specific design and coding of the program. Testing is performed to ensure that the program runs and executes according to its specifications and meet the user's s requirement and expectations .Testing is conducted by executing a program with the intention of uncovering or finding errors. The testing is done by entering test data into the program and subsequently examining the results for any irregularities or unexpected output.

6.1 STEPS IN TESTING PROCESS



University of Malaya

6.1.1 Module Test

Each modules containing logical errors within its boundary were detected in Ciphercrypt by performing module test. The errors within the modules of Ciphercrypt detected and immediately corrected to ensure that all the subroutines and sub functions are error free. Module testing is only conducted after the completion of each program module such as encryption module, authentication module, report module and others.

6.1.2 Function Test

Function test checks that the integrated system performs its function as specified in the requirement. For example, a function test a function test of encrypt function will encrypt all the text and can be viewed by the users.

6.1.3 Performance Test

It compares the integrated components with the nonfunctional system requirement including security, speed and reliability.

6.1.4 Acceptance Test

Acceptance test was done to make sure that the system meets user understanding and requirement which may be differ from the users. For Ciphercrypt, some of my friends were asked to test the system so that they can give their opinion regarding the system.

6.1.5 Installation Test

The installation test was carried out on the PC. This final test is done to ensure that the system is working without any errors.

Debugging is formed as a consequence of successful testing. Testing and debugging are separate activities but all testing activities incorporate debugging. When a test case discover and error, debugging is the process of attempting to match symptom with the cause and if successful, sends to the correction of the error.

The debugging approach employed was the 'cause elimination'. Data related to the error occurrence was organized to to isolate potential causes. A list of all possible causes was developed and test were conducted to eliminate each cause. If initial tests indicate that a particular cause is the culprit, all the data is refined in an attempt to isolate the error.

University of Malaya

7.0 CONCLUSION

7.1 SYSTEM STRENGTHS

Ciphercrypt was created to have a variety of advantages, the following are the strengths of Ciphercrypt:

1. Simple Interface

Ciphercrypt only has a simple interface & few screens. There are also an effective use of buttons that eliminates typing needs for the users. So this will also proved that Ciphercrypt is really a user friendly system.

2. Window Platform

Ciphercrypt was develop to run or operate on Windows platform. This gives the program alarger user manual as well as better response and acceptance since the window platform is the most common and popular used by people.

University of Malaya

3. Strong Encryption Algorithm

The 3-DES encryption algorithm in Ciphercrypt can be considered to be strong. There's a common arithmetic function, XOR functions module function and others in 3-DES. One keyword is required for keyword hash functions. The hashed result will be used with the encryption algorithm to create a strong encrypted output that can't be easily decrypted.

4. Encrypting/Decrypting Option

The above options are provided. Users can encrypt/decrypt the data or files by clicking the encrypt/decrypt button.

5. Encrypt/Decrypt Files Are Automatically Created

Both of the files are automatically created after the original file is encrypted/decrypted. It can also be viewed on a bigger screen by clicking at view button if the space provided on the main screen is not big enough.

6. Various Option On One Interface

On one interface (main interface), all operation can be done. Users don't have to waste their time to go to the next page or the previous one and use this system with ease since they can browse for a file, encrypt / decrypt files, view the output, view the encrypt / decrypt output file just by clicking at the buttons provided.

University of Malaya

7. User Authentication

Ciphercrypt provides user authentication. This mean a user could have to enter the correct username and password before being able to use the application. This is very important to maintain the integrity of Ciphercrypt.

7.2 SYSTEM LIMITATION

There are numbers of limitation in Ciphercrypt . This is because by various features such as the constraints, lack of experience in Visual Basic programming language as well as limited knowledge in the field of Cyphercrypt. The following are the limitations of Ciphercrypt:

1. Stand-Alone System

Ciphercrypt is a stand alone system, not a web based system. This will limit the number of users since they must install the software first before they can use it.

2. No User Feedback

Since it is a stand-alone system, Ciphercrypt cannot gather user feedback for future enhancement.

3. Slow Response Time

The response time for encrypt and decrypt function depends on the size of the document. Larger document take quite a long time to encrypt and decrypt. Sometimes to the extent of causing Ciphercrypt to hang. Therefore, the recommended of a document is anything below 40 lines.

4. Insufficient Help For User

Ciphercrypt is a very simple system. It doesn't support a user interactive help menu and also does not have a step by step user guide .

5. Language Limitations

Only English language is provided in Ciphercrypt system.

6. Limited Functions

Ciphercrypt is lacking in a few of the common functions that are available in most applications such as status bar, font size and type control, etc. Since Ciphercrypt also behaves like a notepad, it should also have the undo and redo function which is very important.

University of Malaya

7.3 FUTURE ENHANCEMENT

Since Ciphercrypt is a prototype model, there's a lot of room for improvement and enhancement. The following are some of the enhancement for the program that will be met in the near future:

1. A Web Based Encryption System

With a web based system, Ciphercrypt will increase the number of users as it is more easier to be accessed.

2. A Web Based System With System Administrator Feature

This feature will enable an administrator t o do remote system administration while away from the server itself. This feature should be included for easy access to the server. It should also contain an administrator username and password to restrict access.

3. User Feedback Feature

This feature can be implemented to increase user interactivity. SQL database would be required to store and retrieve all the information mailed to administrator.

University of Malaya

4. Improve Response Time

Improve the response time for the encrypt and decrypt function by making these functions achieve results much faster compared to the speed of the current version of Ciphercrypt.

5. Provide More Help For User

Ciphercrypt should provide help option with detail explanation and a step by step guide on how to use Ciphercrypt, making it a user interactive one. This help option system must be able to answer related questions by the users.

6. Additional features

Add more functions to Ciphercrypt which are commonly formed in existing program.

University of Malaya

7.4 KNOWLEDGE ACQUIRED

A lot of knowledge has been gained with the development of Ciphercrypt Listed below are of these valuable lessons:

1. Learnt a new programming language (Visual Basic) and many encryption algorithms.
2. Developed skills in fact finding and information gathering.
3. Learnt to work independently, productively and manage the pressure that comes with a certain with a certain task.
4. Improved ability for proper documentation and report writing.
5. Gained experience in problem solving and error checking.
6. Acquired the ability to properly use and manage time.

University of Malaya

SUMMARY

As a final and complete product, Ciphercrypt has achieved all its objectives as well as requirements needed and expected. Ciphercrypt is a stand alone encryption system that able to encrypt and decrypt data consisting of all standard ASCII character.

Ciphercrypt provides strong data encryption with the use of a complex encryption algorithm, DES and keyword hash functionThus, achieving the objective of providing the user with data integrity and security.

Ciphercrypt has a very simple but interactive interfaces and screens. There are encrypt button, decrypt button, view output button,file browsing button and clear screen button on the same interface which is the main screen. The encrypted and decrypted output file are also automatically created right after the user click the encrypt/decrypt button. Users can also view the output in Notepad Window for larger screen. Therefore, the objective of providing a user friendly system has been achieved .

Ciphercrypt also provides user authentication , this will allow the system from being used by unauthorized people.Users need to input the username and password to proceed to the main interface. Even if they've succeed to login other's system, they still need to know the exact keyword used by the owner to ecncrypt/decrypt their files. This feature is vital and can be considered as advantage to Ciphercrypt especially if the user authentication details has been compromised. Therefore, another objective which is the objective of providing system integrity has been achieved.

University of Malaya

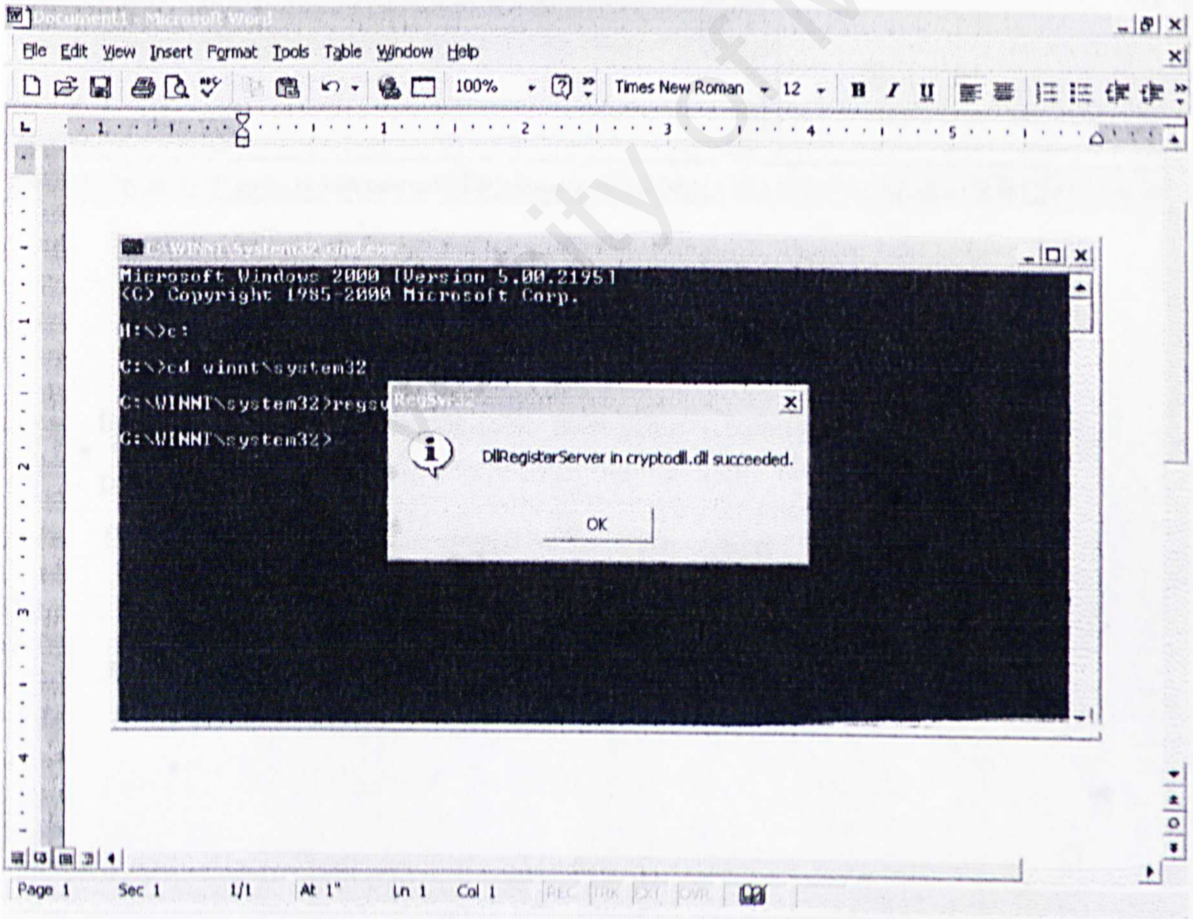
USER MANUAL

- Ciphercrypt must download Cryptodll library first before it can be run

- To download Cryptodll library:-

    1. Start→ Run→Type cmd
    2. The black screen as shown below will appear
    3. Type H:\ >c:
    4. Type C:\>cd winnt\system32>regsvr32 Cryptodll.dll
    5. →Enter

- A successful downloaded Crytodll.dll message (shown in Figure 1.0) will appear
- Ciphercrypt is ready to be run.


Document1 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
100%
Times New Roman
12
C:\WINNT\System32\cmd.exe
RegSvr32
OK
Page 1 Sec 1 1/1 At 1" Ln 1 Col 1 REC TRK EXT OVR

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

H:\>c:

C:\>cd winnt\system32

C:\WINNT\system32>regsv

C:\WINNT\system32>
```

DllRegisterServer in cryptodll.dll succeeded.

Figure 1.0 Cryptodll Library Successfully Downloaded Message

University of Malaya

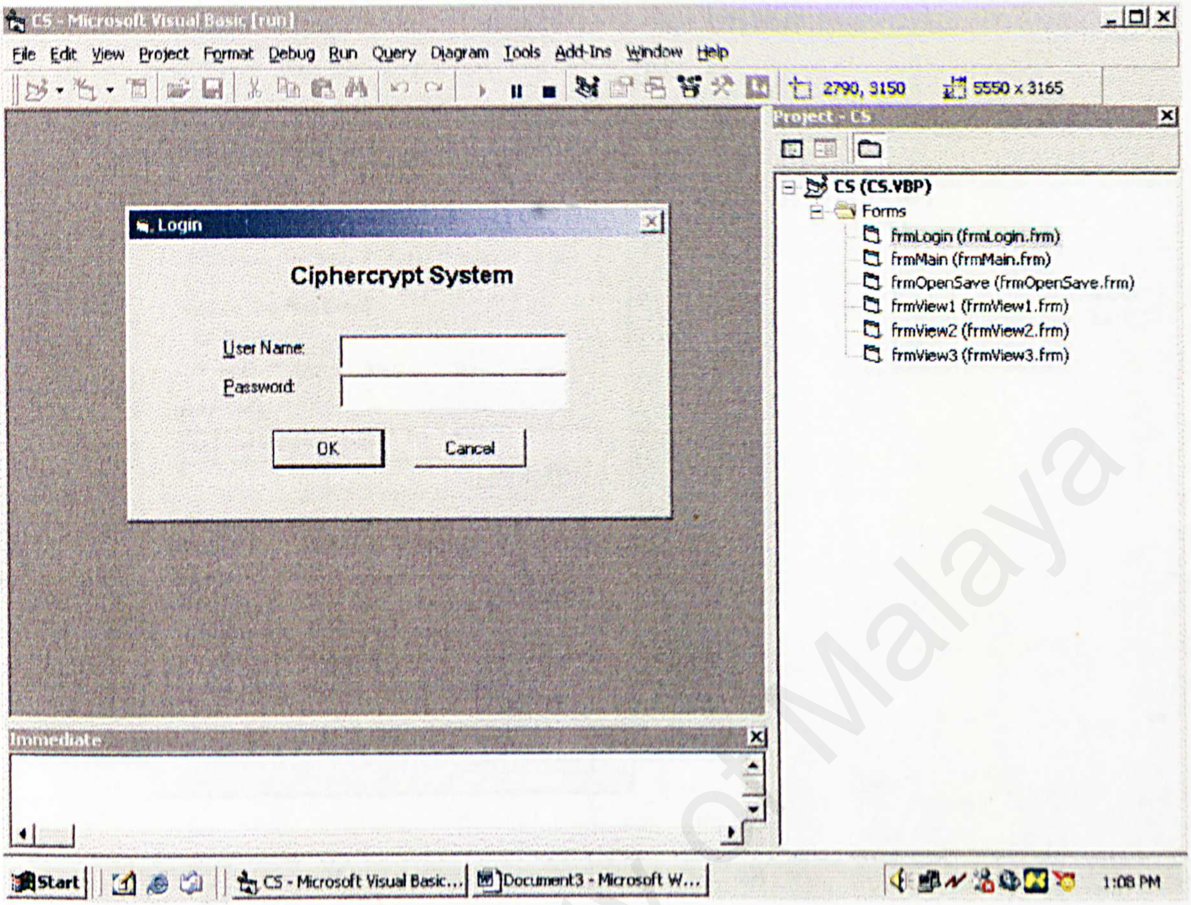
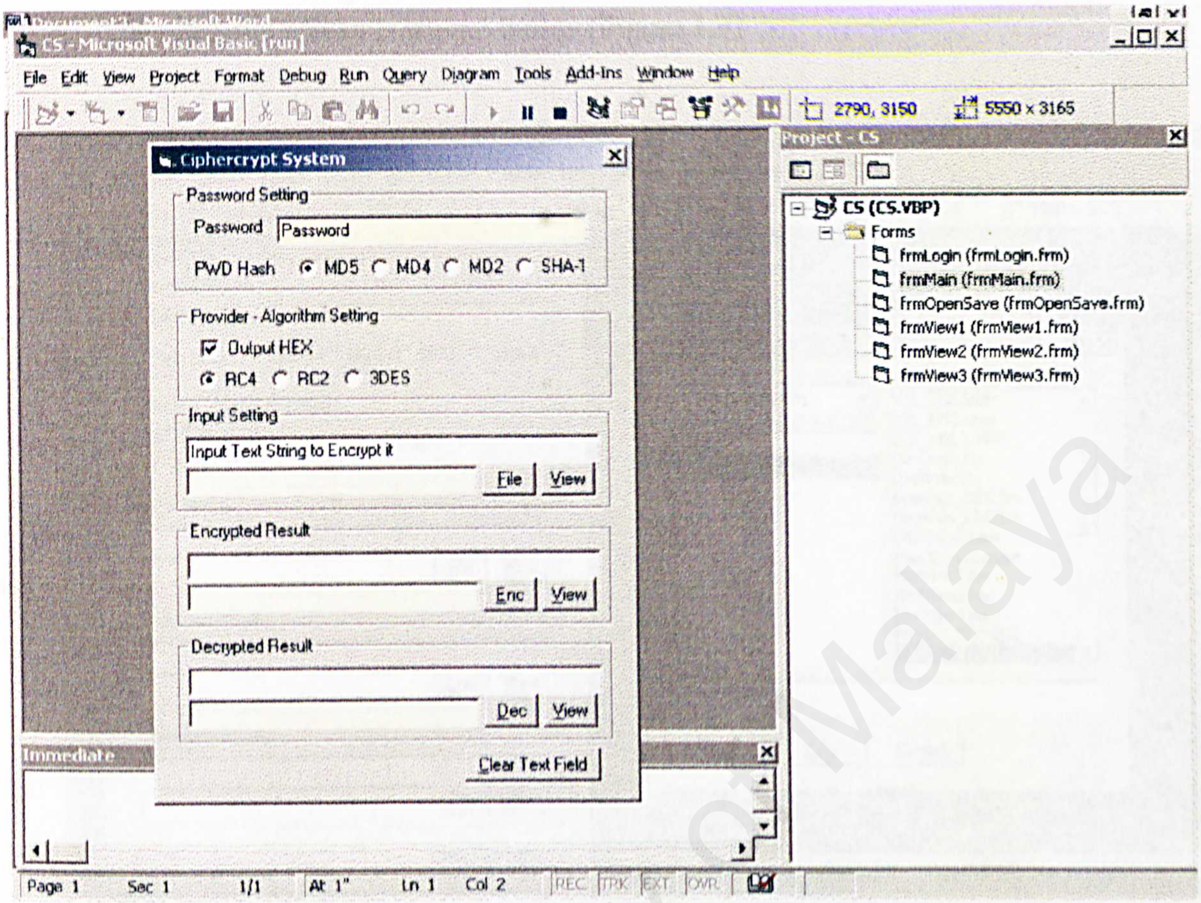


Figure 1.1 Authentication Screen

- In authentication screen, the user must enter a default username (CS) and a password (password)
- This will enable user to proceed to the main screen

University of Malaya



Password Setting

Password: Password

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

Input Text String to Encrypt it

Encrypted Result

Decrypted Result

Figure 1.2 Main Screen

- At Keyword Setting, Enter any words or string of characters to be used in Keyword Hash Function.

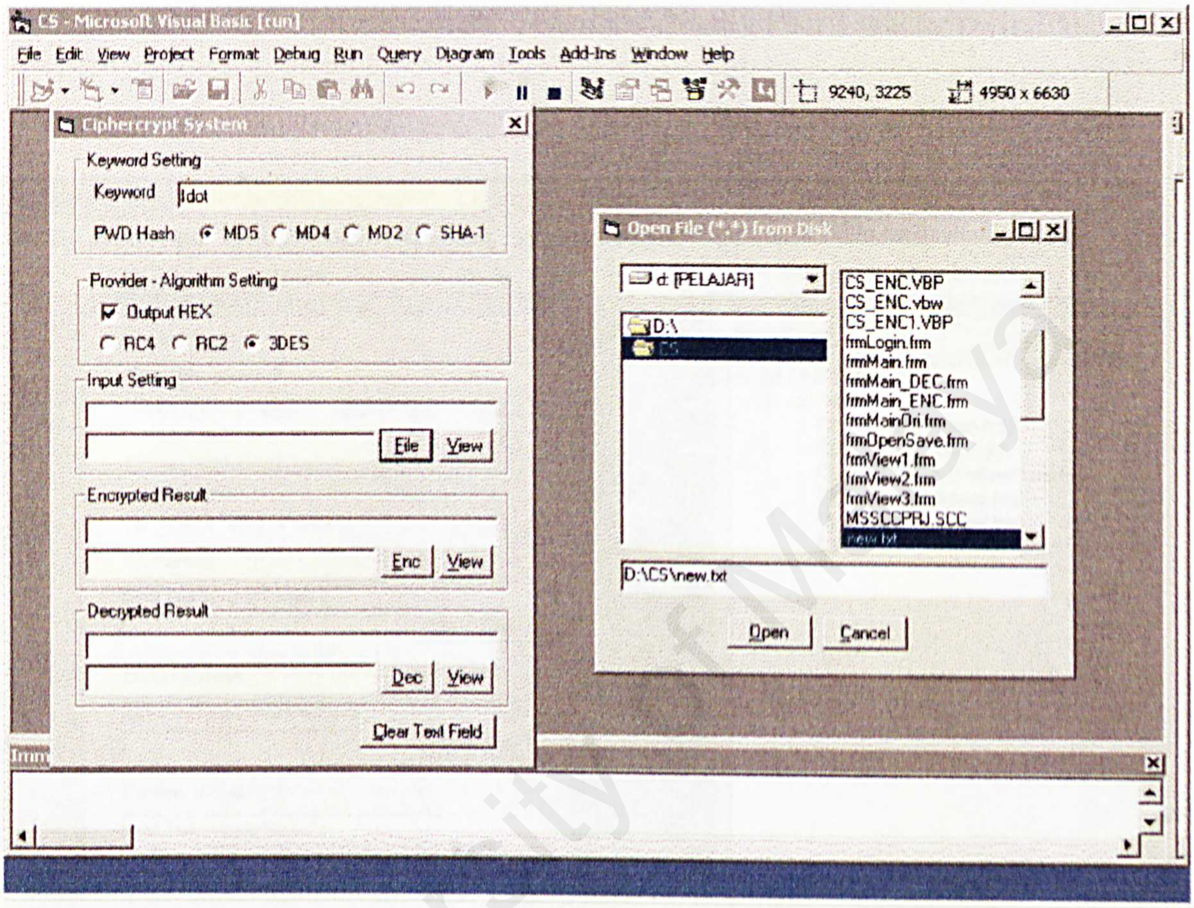
- Then select an encryption algorithm setting. User can either choose RC4, RC2 or 3 DES algorithm.

- Input Text string or to be encrypted.

- To encrypt a file click at file button to browse for an existing file.

University of Malaya

- The open file screen is shown below (Figure 1.3)


CS - Microsoft Visual Basic [run]

Ciphercrypt System

Keyword Setting

Keyword: ldot

PWD Hash: ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

○ RC4 ○ RC2 ● 3DES

Open File (*.*) from Disk

d: [PELAJAR]

D:\
CS

CS_ENC.VBP
CS_ENC.vbw
CS_ENC1.VBP
frmLogin.frm
frmMain.frm
frmMain_DEC.frm
frmMain_ENC.frm
frmMainOri.frm
frmOpenSave.frm
frmView1.frm
frmView2.frm
frmView3.frm
MSSCCPRJ.SCC
new.txt

D:\CS\new.txt

Figure 1.3 Open File Screen

- Click open after a file is selected. Click cancel to cancel browsing for a file.

- Click encrypt to encrypt and decrypt button to decrypt the file.

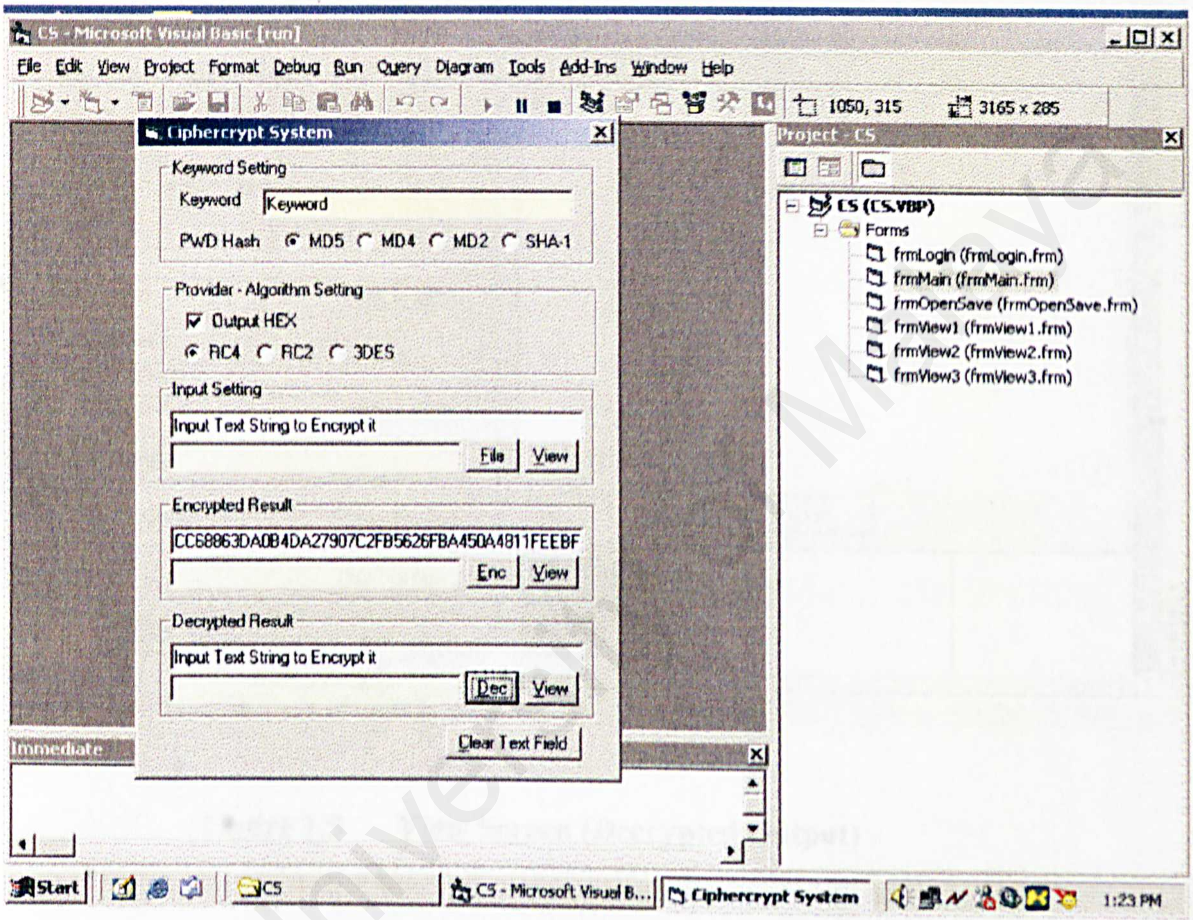
- To view the encrypted file, click view button next to encrypt button.

- To view the decrypted file, click view button next to decrypt button.

University of Malaya

- To view the original file, click view button next to file button.

- Clear Text File button is used to clear all the file and do another encryption/decryption process.



Keyword Setting

Keyword: Keyword

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

Input Text String to Encrypt it

Encrypted Result

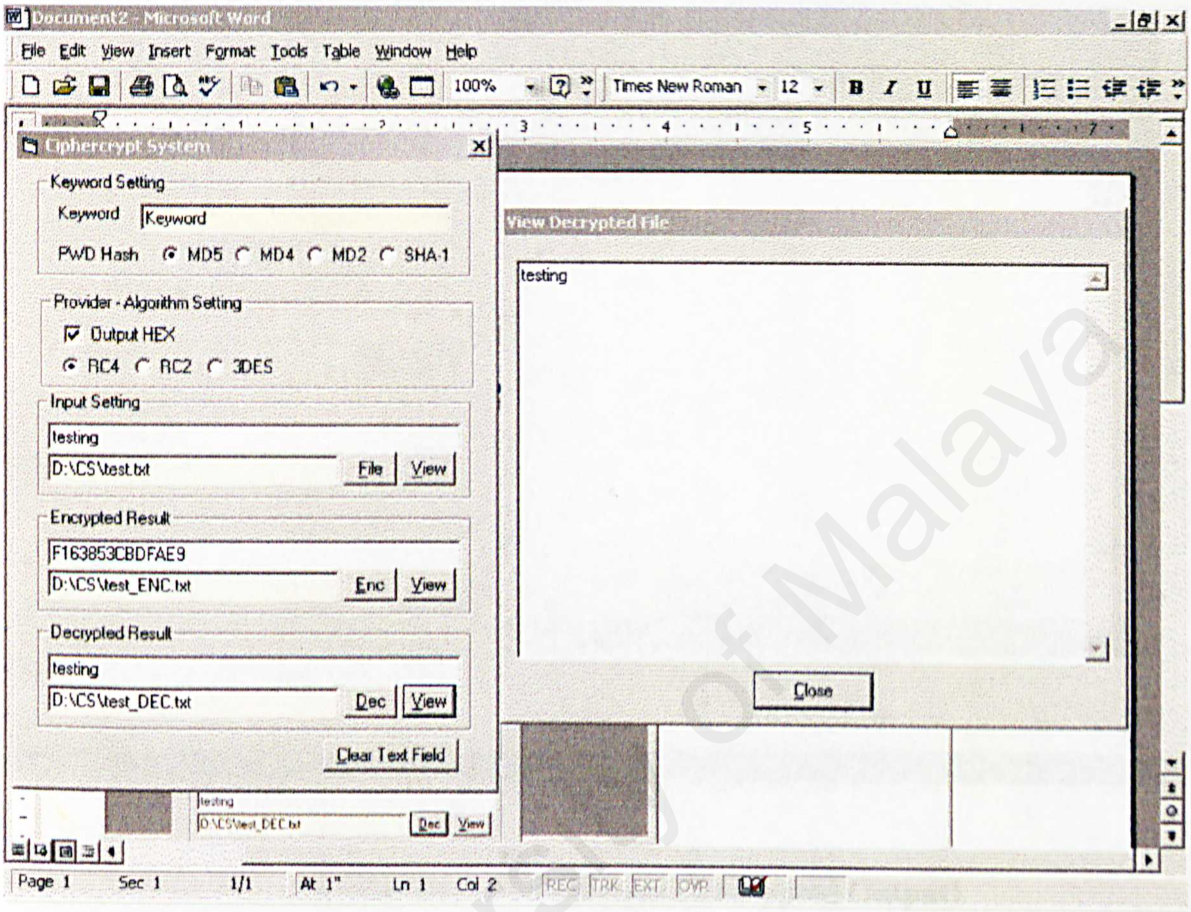
CC68863DA0B4DA27907C2FB5626FBA450A4811FEEBF

Decrypted Result

Input Text String to Encrypt it

Figure 1.4 String Encrytion/Decryption

- An example of encrypted /decryted output (in string form) in Figure 4.24


Document2 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
100%
Times New Roman 12
Ciphercrypt System
File View
Enc View
Dec View
Clear Text Field
View Decrypted File
Close
Page 1 Sec 1 1/1 At 1" Ln 1 Col 2 REC TRK EXT OVR

Keyword Setting

Keyword: Keyword

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

testing

D:\CS\test.txt

Encrypted Result

F163853CBDFAE9

D:\CS\test_ENC.txt

Decrypted Result

testing

D:\CS\test_DEC.txt

View Decrypted File

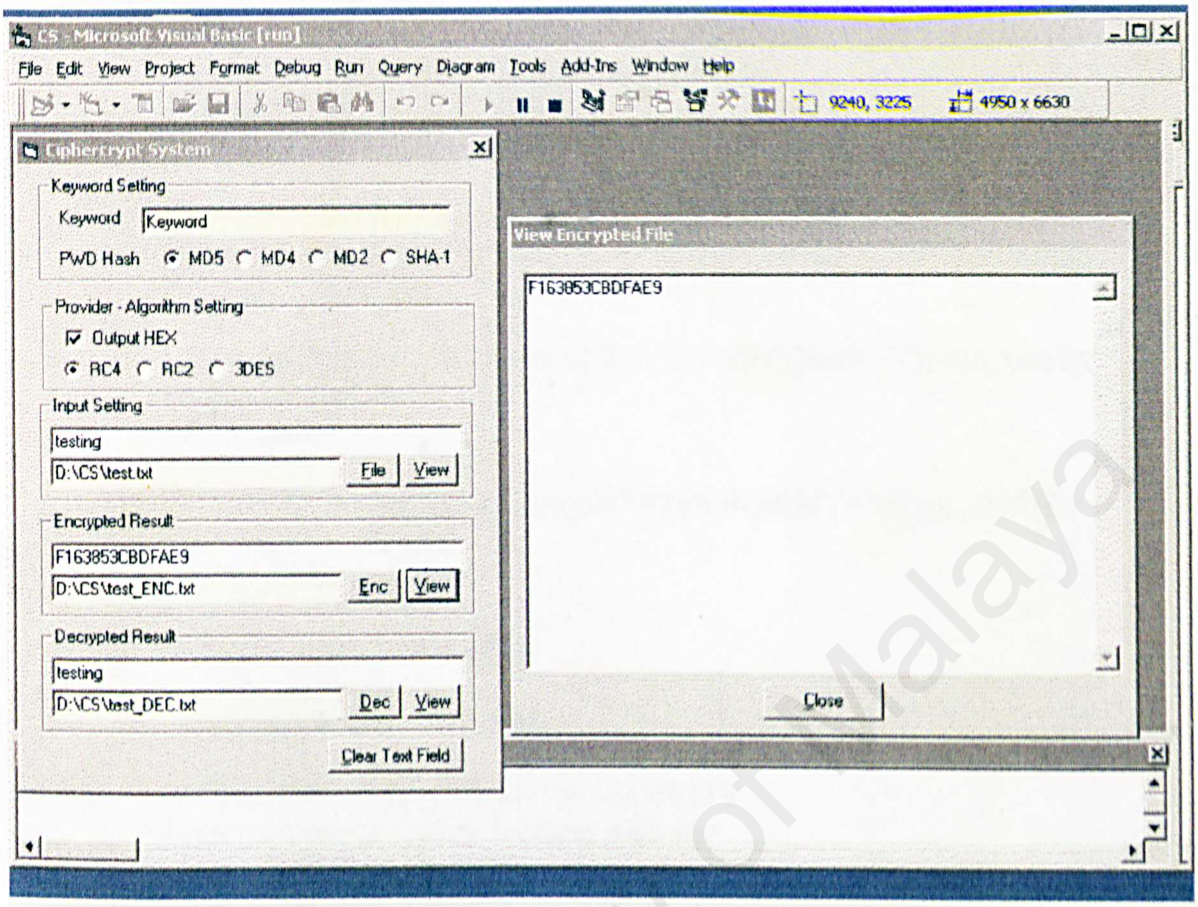
testing

Figure 1.5 View Screen (Decrypted Output)

- Users can also view the decrypted file in view screen beside viewing at the main screen

- Click the Close button to close the view screen

University of Malaya


CS - Microsoft Visual Basic [run]
File Edit View Project Format Debug Run Query Diagram Tools Add-Ins Window Help
9240, 3225
4950 x 6630
Ciphercrypt System
File
View
Enc
View
Dec
View
Clear Text Field
View Encrypted File
Close

Keyword Setting

Keyword: Keyword

PWD Hash ● MD5 ○ MD4 ○ MD2 ○ SHA-1

Provider - Algorithm Setting

☑ Output HEX

● RC4 ○ RC2 ○ 3DES

Input Setting

testing

D:\CS\test.txt

Encrypted Result

F163853CBDFAE9

D:\CS\test_ENC.txt

Decrypted Result

testing

D:\CS\test_DEC.txt

View Encrypted File

F163853CBDFAE9

Figure 1.6 View Screen (Encrypted Output)

- Users can also view the encrypted file in view screen beside viewing at the main screen
- Click the Close button to close the view screen

University of Malaya

BIBLIOGRAPHY

BOOKS

1. CRYPTOGRAPHY & NETWORK SECURITY
   Principles & Practice (2nd Edition)
   By William Stalling Prentice Hall

2. SECURITY & PRIVACY IN COMPUTER SYSTEM
   Melville Publishing Company
   By Lance J. Hoffman

3. CRYPTOGRAPHY-AN INTRODUCTION TO COMPUTER SECURITY
   By Josef Pierpryzk
   Prentice Hall

4. DEVELOPING APPLICATION WITH MICROSOFT VISUAL BASIC
   By Michael V. Ekedahl
   Course Technology Inc.

5. APPLIED CRYPTOGRAPHY
   By Bruce Schneier,
   John Wiley & Sons, New York

6. CRYPTOGRAPHY AND DATA SECURITY
   Dorthy Elizabeth Robling Denning Addison
   Wesley Publishing Company

WEBSITES

1. http://www.rsa.com/rsalabs/97challenge/.

2. http://www.cipherbritters.com

3. http://www.aspsimply.com

4. http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/top.html.

5. http://www.fortify.net/related/cryptographers.html

University of Malaya