DATA TRANSMISSION USING AES ENCRYPTION VIA EMAIL AND SMS

ARIF HANAFI BIN SHARIF KATULLAH

A thesis submitted in fulfillment of the requirements for the award of the degree of the Bachelor of Computer Science (Software Engineering)

FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING
UNIVERSITY MALAYSIA PAHANG

2013
ABSTRACT

A computer, and other mobile computing devices, are generally accepted globally as a personal computing platform. Given the amount of sensitive information gathered by these devices, there are serious privacy and security implications for both individual use and enterprise organization. Confidentiality of the data can be effectively restricted by deploying an encryption file technique. All major computers Operating System now integrates some form of encryption. In certain situations, this is inadequate, as users may be forced into disclosing their decryption keys. In this case, the data must be hidden so that it is very certainly transmit sensitive information but unable to intercept easily if not encrypt before sending to the intended person. Encryption and decryption technique while the interior structure's strength of the data file depends on the key/password it used. This thesis priority is to avoid the using of the manual process such as hand-to-hand method transmission while maintaining the concealment of their sensitive or confidential data and explores the usefulness of encryption for computer devices. Users especially choose weak technique. The goal is to ensure the confidential data is not reachable for unauthorized personnel by implementing the use of passwords that are for encryption keys and to make ease for the transmission confidential data via email platform.
**ABSTRAK**

Table of Content

DECLARATION ...........................................................................................................II

SUPERVISOR DECLARATION..................................................................................III

ACKNOWLEDGEMENT..............................................................................................IV

ABSTRACT..................................................................................................................V

ABSTRAK...................................................................................................................VI

LIST OF TABLES.......................................................................................................X

LIST OF FIGURES....................................................................................................XI

LIST OF APPENDIX .................................................................................................XIII

CHAPTER 1.................................................................................................................1

INTRODUCTION .......................................................................................................1
  1.1 BACKGROUND ....................................................................................................1
  1.2 PROBLEM STATEMENTS ....................................................................................4
  1.3 OBJECTIVES .....................................................................................................4
  1.4 SCOPE OF STUDY ...............................................................................................5
  1.5 TERMINOLOGY ..................................................................................................5
  1.6 THESIS ORGANIZATION ...................................................................................6

CHAPTER 2.................................................................................................................7
LITERATURE REVIEW ........................................................................................................... 7
2.0 INTRODUCTION .................................................................................................................. 7
2.2 COMPARISON BETWEEN CRYPTOGRAPHIC TECHNIQUES ................................................... 9
2.3 WHY AES? ............................................................................................................................. 11
2.4 TYPES OF CRYPTOGRAPHY ............................................................................................... 11
2.5 EXISTING OF AES DATA-ENCRYPTION SYSTEM ................................................................. 12
2.5.1 FOLDER LOCK 6.4.1 ......................................................................................................... 12
2.5.2 ADVANCED ENCRYPTION PACKAGE PRO 5.3.6 ............................................................... 15
2.5.3 SECUREIT 4.2.0............................................................................................................... 18
2.5.4 SENSIGUARD 3.1 ............................................................................................................. 20
2.6 COMPARISON BETWEEN EXISTING SYSTEM AND THE PROTOTYPE ................................... 23
2.7 TECHNIQUE ......................................................................................................................... 25
2.7.1 STAND ALONE WINDOWS APPLICATION ................................................................... 25
2.7.2 GSM MODEM .................................................................................................................. 25
2.7.3 ADVANCED ENCRYPTION STANDARD .......................................................................... 26
2.7.3.1 ENCRYPTION .............................................................................................................. 28
2.7.3.2 DECRYPTION .............................................................................................................. 30
2.7.3.3 AES CIPHER FUNCTION .......................................................................................... 31

CHAPTER 3 ................................................................................................................................. 44

METHODOLOGY ....................................................................................................................... 44
3.1 INTRODUCTION OF METHODOLOGY ............................................................................. 44
3.2 PROJECT METHODOLOGY ................................................................................................... 45
3.3 REQUIREMENT PLANNING PHASE ....................................................................................... 48
3.3.1 PLANNING ......................................................................................................................... 49
3.3.2 ANALYSIS REQUIREMENT ............................................................................................... 49
3.4 USER DESIGN PHASE .......................................................................................................... 49
3.4.1 PROTOTYPE FLOWCHART ............................................................................................... 50
3.4.2 USE CASE ......................................................................................................................... 51
3.4.3 USER INTERFACE ............................................................................................................. 53
3.5 CONSTRUCTION PHASE

3.6 CUTOVER PHASE

CHAPTER 4

IMPLEMENTATION

4.1 INTRODUCTION

4.2 TOOLS AND TECHNOLOGIES

4.2.1 DEBUGGING AND RUNNING THE SYSTEM

CHAPTER 5

RESULTS AND DISCUSSION

5.1 EXPECTED RESULTS

5.2 DISCUSSION

5.3 PROJECT CONSTRAINT

5.3.1 DEVELOPMENT CONSTRAINT

5.4 ADVANTAGES AND DISADVANTAGES OF THE SYSTEM

CHAPTER 6

CONCLUSION AND FUTURE WORKS

6.1 CONCLUSION

6.2 FUTURE SUGGESTION

REFERENCES

APPENDIX A
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Comparison of encryption techniques</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Comparison between existing system and the prototype</td>
<td>23</td>
</tr>
<tr>
<td>2.3</td>
<td>Table of round</td>
<td>27</td>
</tr>
<tr>
<td>2.4</td>
<td>AES encryption cipher using 16 byte key</td>
<td>28</td>
</tr>
<tr>
<td>2.5</td>
<td>AES encryption cipher using 24 byte key</td>
<td>29</td>
</tr>
<tr>
<td>2.6</td>
<td>AES encryption cipher using 32 byte key</td>
<td>29</td>
</tr>
<tr>
<td>2.7</td>
<td>AES decryption cipher using 16 byte key</td>
<td>30</td>
</tr>
<tr>
<td>2.8</td>
<td>AES decryption cipher using 24 byte key.</td>
<td>30</td>
</tr>
<tr>
<td>2.9</td>
<td>AES decryption cipher using 32 byte key</td>
<td>31</td>
</tr>
<tr>
<td>2.10</td>
<td>The first time Add Round Key gets executed</td>
<td>32</td>
</tr>
<tr>
<td>2.11</td>
<td>The second time Add Round Key is executed</td>
<td>32</td>
</tr>
<tr>
<td>2.12</td>
<td>E Table</td>
<td>38</td>
</tr>
<tr>
<td>2.13</td>
<td>L Table</td>
<td>38</td>
</tr>
</tbody>
</table>
3.1 Hardware Requirement 56
3.2 Software Requirement 56

LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Interface of Folder Lock 1</td>
<td>13</td>
</tr>
<tr>
<td>2.2</td>
<td>Interface of Folder Lock 2</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>Interface of Folder Lock 3</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>Interface of Folder Lock 4</td>
<td>14</td>
</tr>
<tr>
<td>2.5</td>
<td>Interface of Advanced Encryption Package Pro 5.3.6</td>
<td>1</td>
</tr>
<tr>
<td>2.6</td>
<td>Interface of Advanced Encryption Package Pro 5.3.6</td>
<td>2</td>
</tr>
<tr>
<td>2.7</td>
<td>Interface of Advanced Encryption Package Pro 5.3.6</td>
<td>3</td>
</tr>
<tr>
<td>2.8</td>
<td>Interface of SecureIT 4.2.0</td>
<td>1</td>
</tr>
<tr>
<td>2.9</td>
<td>Interface of SecureIT 4.2.0</td>
<td>2</td>
</tr>
<tr>
<td>2.10</td>
<td>Interface of SecureIT 4.2.0</td>
<td>3</td>
</tr>
<tr>
<td>2.11</td>
<td>Interface of SensiGuard 3.1</td>
<td>1</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.12</td>
<td>Interface of SensiGuard 3.1</td>
<td>2</td>
</tr>
<tr>
<td>2.13</td>
<td>Interface of SensiGuard 3.1</td>
<td>3</td>
</tr>
<tr>
<td>2.14</td>
<td>AES Forward Cipher Flow Graph</td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>RAD Methodology</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>The four phases of the RAD model</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Flowchart</td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Use case diagram</td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>Data encryption and decryption interface</td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>Send password or any remarks, using SMS</td>
<td></td>
</tr>
<tr>
<td>3.7</td>
<td>Email platform with attachment interface</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>The running state of encryption process</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>The running state of decryption process</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>SMS platform</td>
<td></td>
</tr>
</tbody>
</table>
LIST OF APPENDIX

APPENDIX

A

FUNCTION CODING
CHAPTER 1

INTRODUCTION

This section briefly describes the entire overview research that includes five parts. Foremost, is the introduction, followed by the problem statement. Then, is the objective and of study. Finally terminology and thesis organization.

1.1 Background

The desire to transmit messages securely is not new for centuries. Community kept communication secret. Nowadays, with the latest technology, particularly the Internet vast amount data transmit sensitive data such as confidential trade secrets, military strategies and Government communication (Eskicioglu, 2001).

Encryption is the main key structure to prevent malicious attacks and is an essential role of Information Security. However, providing the alternative in information privacy, but it acts as authenticate coming from the sender. As a result, the rationale of adopting the correct encryption techniques is vital the reliability of data may be leaked once weakness in the encryption key was detected by preventing tampering, falsification and counterfeiting. Transmitting messages is not new for centuries community continues look way or method to transmitted data with efficient and optimizes time. Encryption and decryption technique security heavily relied on the interior structure of the strength depend on the key it uses (Xin et al, 2011). Cryptography or secret codes have been known some 4000 years.
Now, first being used by the ancient Egyptians, the prospect of writing something that only selected persons can decipher has proven its usefulness through many years. Cryptography has played decisive roles in both World War I and II (Maartmann-Moe, 2007). This deployment is not new since ancient times, Julius Caesar (100 B.C.E. – 44 B.C.E) employed by sending secret messages. This method is shift performed modular 26. The plaintext A become D, B became E and Z substitute to C (Eskicioglu, 2001). Figure 1.1 describes how plaintext encrypted becomes a cipher text before been transmitted to insecure channel. After receiving the cipher text it needs to be decrypted before it able to get the plaintext.

Many times when sensitive data is exchanged electronically the privacy of the data is a requirement. The use of encryption restricts unintended receivers from viewing the confidential data, which are deemed confidential and potentially dangerous if made known to irresponsible persons. Today, encryption is the procedure of transforming plaintext, data that can be read by anyone, to cipher text, data that can only be read by someone with a secret decryption key. A message before being changed in any way is called plaintext. Plaintext messages are converted to cipher text via some encryption method. A particular such method is called a cryptosystem. Cryptosystem would be a suitable method in implement to the examination paper (confidential data) to avoid any sensitive data fall into someone else that not involve.

A cryptosystem is designed so that decryption can be accomplished only under certain conditions, which generally means only by persons in possession of both a decryption engine (these days, generally a computer program) and a particular piece of information, called the decryption key, which is supplied to the decryption engine in the process of decryption. Plaintext is converted into cipher text by means of an encryption engine (again, generally a computer program) whose operation is fixed and determinate (the encryption method) but which functions in practice in a way dependent on a piece of information (the encryption key) which has a major effect on the output of the encryption process. A cryptosystem could be
designed which made use of several different methods of encryption, the particular method chosen for a particular encryption process being key-dependent.

The combination of encryption methods results again in an encryption method, which is just as deterministic as a simpler cryptosystem, although probably harder for a cryptanalyst to crack. A good cryptosystem should in fact vary the details of its encryption method in a key-dependent way, though high security does not require the combination of distinct encryption algorithms. The result of using the decryption method and the decryption key to decrypt cipher text produced by using the encryption method and the encryption key should always be the same as the original plaintext (except perhaps for some insignificant differences). In this process the encryption key and the decryption key may or may not be the same.

The Advanced Encryption Standard, in the following referenced as AES, is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard was found too weak because of its small key size and the technological advancements in processor power. Fifteen candidates were accepted in 1998 and based on public comments the pool was reduced to five finalists in 1999. In October 2000, one of these five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndael. The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a Block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size.

The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192 and 256 bits. While AES supports only block size of 128 bits and key sizes of 128, 192 and 256 bits, the original Rijndael supports key and block sizes in any multiple of 32, with a minimum of 128 and a maximum of 256 bits.
1.2 **Problem Statements**

The confidential data that are involved in assembling or transferring the confidential data still using the traditional method (manual process hands-to-hands). The confidential data that process manually leads to the exposing of human errors, this problem can produce the security issues. What if the papers that contain confidential information were lost and possessed by irresponsible person it would jeopardize the integrity of the data itself. The manual process should develop a good security and only the authorized personnel can access the confidential data when the process of preparing examination takes place. The security of the manual process is still in uncertainty in how the organization accomplishes the examination paper security in each process. When there are changes in the examination question the manual process of transferring confidential data also creates a difficulty to lecturers to get seat with the panel for the vetting process and evaluation session when they are in a different time and place.

1.3 **Objectives**

In this section the objectives of the project will be clear out. Thus, the objectives of this project are as follows:-

- To develop a prototype that encrypts the confidential files.

- To employ an AES encryption technique in the process of transferring confidential files.

- To test the propose prototype in order to evaluate the provided functions able to execute smoothly.
1.4 Scope Of Study

- The main scope of the prototype is to encrypt the confidential data file (personal data, credit card data, examination paper and many more).
- This system is developed by using VB.net language and using GSM Modem in the application that run on Windows.
- The file extension that can be encrypted/decrypted (.doc, .txt, .pdf, .png, jpeg, jpg)
- The SMS and E-mail can be sent directly when using the system

1.5 Terminology

Web-Based

- A web application is an application that is accessed over a network such as the Internet or an intranet

Encryption

- The activity of converting data or information into code.

Cryptanalysis

- Science and sometimes art of breaking cryptosystems.

Cryptosystem

- System for encoding and decoding secret messages
1.6 Thesis Organization

This thesis consists of six (6) chapters.

**Chapter 1** will discuss on introduction to the system. The discussion consists of system overview. Problem statement discuss on the problem that faced by the current system. On objectives, the reasons of the development of project are listed. Scope of the project is discussed on project and user limitation.

**Chapter 2** is literature review which will discuss on current system and the technique or software that is used in the current system.

**Chapter 3** will discuss on system methodology. It will be discuss on the method that is used to develop the system and project planning. In this chapter also will discuss the needs of the project such as the software and the device that are needed to develop the system.

**Chapter 4** will discuss on project implementation. This chapter will discuss on design of project development.

**Chapter 5** will discuss on the discussion and result that receive from the data and data analysis, project constrains and, fix and suggestion of the system. Project analysis will discuss on project objective which continuously with project problem.

**Chapter 6** will discuss on conclusion of the project. This is including the conclusion of the data that are received and conclusion of the methodology and used research implementation.
CHAPTER 2

LITERATURE REVIEW

2.0  Introduction

The purpose of reviewing previous work is to guide through the kind of work that others have done related to the project field. A literature review is a body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological offerings to a particular topic. This chapter will take brief explanations on study of previous or existing system that related to the proposed system, based on the development process, tools and platform used.

Many technologies exist that can be adapted in order to integrate a stand-alone system. By making a research and analyze the system strength and weaknesses, it will be easier to me developed system for AES data encryption system. An encryption process uses an algorithm and a key to transform plain text which is original data into cipher text. The inverse of the encryption process is decryption. Only people who have the secret key or password can decrypt the message into plain text encrypted messages can sometimes be broken by cryptanalysis, which is also called code breaking although modern cryptography techniques are virtually unbreakable electronic security becomes increasingly important as nowadays the internet and other forms of electronic communication become more prevalent and not secure. It is the technique of the principle means to protect information security. Besides ensuring the information is confidential, it also
provides digital signature, authentication, secret sub-storage, system security and any other functions

2.1 Overview of Data File Transmission Using AES Encryption via Email and SMS

Currently the transferring confidential data for FSKKP faculty still using hands-to-hands method. This might lead to the exposing the human errors if the staff that handle the confidential data lost or misplaced it. The system that will develop will be able to encrypt the data using the user own password or secret key. The users that key-in the password should take great care when the users select the password because the prototype has no way to retrieve a lost password. The user can send the password to the person they want straightly to receiver mobile by insert the receiver mobile phone number. The user also can send the data that is fully encrypt via email platform that is also provide in the system. This encryption system used 256-bit Advanced Encryption Standard (AES) method. When the receiver received the encrypted files the receiver can open the files by using the password that was sent via mobile. This will provide a good security level for the confidential files. The prototype will protect the confidential and the integrity of the files.
2.2 Comparison between cryptographic techniques

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher. 3DES is an enhancement of DES it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods (Coppersmith, D. 1994).

RC2 is a 64-bits block cipher with a variable key size that range from 8 to 128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts (Coppersmith, D. 1994).

Blowfish is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable-length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to Twofish.

AES is a block cipher. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications. The cipher key used in the algorithm is of 128 bits. Therefore, to break the cipher key an attacker has to check 2^128 possibilities which are practically almost impossible. Therefore, the brute-force attack fails on this algorithm. The flow of the algorithm makes sure that there is no fixed pattern in any of the steps of the algorithm. The components of the proposed algorithm have brought about strong diffusion and confusion. Therefore, statistical and pattern analysis of the ciphertext fails. The most important security advantage is that no differential or linear attacks can break this algorithm (Rayarikar et al, 2012).
RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard (Khate, 2009).

Table 2.1: Comparison of encryption techniques

<table>
<thead>
<tr>
<th>Factors</th>
<th>AES</th>
<th>3DES</th>
<th>DES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Length</td>
<td>128, 192 or 256 bits</td>
<td>(k1, k2 and k3) 168 bits</td>
<td>56 bits</td>
</tr>
<tr>
<td>Cipher Type</td>
<td>Symmetric</td>
<td>Symmetric</td>
<td>Symmetric</td>
</tr>
<tr>
<td>Block Size</td>
<td>128, 192 or 256 bits</td>
<td>64 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>Developed</td>
<td>2000</td>
<td>1978</td>
<td>1977</td>
</tr>
<tr>
<td>Cryptanalysis</td>
<td>Strong to any attack</td>
<td>Vulnerable in some attacks</td>
<td>Vulnerable</td>
</tr>
<tr>
<td>Resistance</td>
<td>Considered Secured</td>
<td>Intermediate</td>
<td>Proven inadequate</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible Keys</td>
<td>$2^{128}$, $2^{192}$ and $2^{256}$</td>
<td>$2^{112}$ and $2^{168}$</td>
<td>$2^{56}$</td>
</tr>
<tr>
<td>Time Require to check keys at 50 billion keys per second</td>
<td>For 128 bits = $5 \times 10^{21}$ years</td>
<td>For 112 bit key = 800 days</td>
<td>For 56 bit keys = 400 days</td>
</tr>
</tbody>
</table>
2.3 Why AES?

The latest trends in e-mail system that utilize handling of two categories cryptographic (RSA by means of asymmetric keys and AES through symmetric key). These methods build a strong encryption base capable of enduring numerous types of hit, uncovering and reverse engineering. The computer which using AES 128 bit was designed to negate the major defect existing in other encryption communication (Hopper et al 2009 and Yang 2006). The AES may remain the undisputed encryption process that able to withstand the entire process of the "weakest link in the encryption" both leave behind several stages of protection (Mare et al, 2011).

2.4 Types of cryptography

Willingly available are numerous conduct of sort cryptographic techniques. At this point value amount of keys that use for encryption and decryption. The two types of techniques are:

a) Secret key cryptography - occasionally known as symmetric cryptography. It long-established form of cryptography, single key used to encrypt and decrypt a message. In some situation not only handle encryption, but also conformity with authentication. These techniques were used by message authentication codes (Kaufman et al, 2002).

b) Public Key Encryption - Most noteworthy recent growth cryptography the last few centuries was mentioned by Stanford University lecturer Martin Hellman along with Graduate apprentice Whitfield Diffie in 1976. Their research about possible that both users can exchange different key via secure communiqué over a secure communications outlet as private key not make known other party (Kaufman et al,2002).
2.5 Existing of AES data-encryption system

This part will describe briefly any existing system that using the same technique of encryption that is available in the website. The users need to purchase the product to use any of the existing system in the online website.

2.5.1 Folder Lock 6.4.1

Folder Lock's security is robust with 256 bit AES encryption. Decryption was transparent and showed no signs of lag even when playing a 1.7GB video file. The original files are shredded after encryption, leaving no remains on the user's PC, and file integrity was maintained after decryption. To insure a quality password is chosen, a password meter is displayed as a red or green ring around the safe’s combination dial, providing immediate feedback regarding the password’s strength. Should the user decide not to create a password, the password generator utility will securely accomplish the task.

The virtual keyboard method for inputting passwords prevents key-loggers from capturing key presses from the keyboard; an advanced security precaution utilized by many online banks. Another enhancement is that the “lockers,” which contain all your files, cannot be deleted unless the password is known. This prevents others from destroying your data, whether intentional or not. Some right click context menu options lets the user choose whether to “lock” or “encrypt” the files or folders. Both methods ensure the data is well protected. The history cleaning option can remove document history and clear clipboard data, which is an added bonus for this type of software. Stealth mode can completely hide the program from Windows and can be engaged with a user definable hot key.

Folder Lock is an easy-to-use encryption software package. After a short setup of creating a new locker, accessing files and folders is a breeze and there is no noticeable slowdown when accessing your data. The many security features of this software set it apart from all the other encryption programs. One gem is the portability feature of Folder Lock, which allows you to take all your files on-the-go, for example, transferring your locker to a USB drive. After creating a locker, you
merely select the portability button, which creates an auto run executable file and moves both to the USB drive. This creates a mini version of Folder Lock, and can be used on any Windows computer without the original software.

This usage limit doesn't give a user enough experimentation time to try all the features. In addition, when right clicking on files or folders, sometimes the folder lock option was available, other times it was not. Lastly, the software was often slow when opening and closing, but was still 100% functional.

**Figure 2.1 : Interface of Folder Lock 1**

As shown in the figure above the auto protection option can be toggled on or off. If turned on, it can be set from 5 to 360 minutes of idle time to protect your locker.
Figure 2.2: Interface of Folder Lock
As shown in the figure above the hack attempt monitoring feature checks for 5 consecutive fake password attempts. It can be set to either log off the PC or shut it down.

Figure 2.3: Interface of Folder Lock
The figure above shows the history cleaning window will remove unwanted traces from your computer. It's limited to clearing recent document history, files and folder history and clipboard data. Further cleaning requires purchase of a separate product.

Figure 2.4: Interface of Folder Lock
The figure above shows select the files you want to encrypt from the mini explorer window. Drag to the vault, and once you see them there, click "encrypt". This move