PROJECT TITLE: DESIGN AND IMPLEMENTATION OF AN ENCRYTED DAIRY

BY NWAGBOSO CHUKWUEMEKA CHINEDU

A DISSERTATION PRESENTED TO THE FACULTY OF ………………………………………………………………………………………………………

W**yższa Szkoła Informatyki i Umiejętności**

IN CANDIDACY FOR THE DEGREE

BACHELOR OF SCIENCE

RECOMMENDED FOR ACCEPTANCE

BY THE DEPARTMENT OF

COMPUTER SCIENCE

**ACKNOWLEDGEMENT**

It is my profound pleasure to express my deep sense of gratitude to the Almighty God for granting me the strength to successfully complete my project.

Big thanks to the Department of Computer Science Wyzsza Szkola Informatyki I Umiejetnosci and that of Babcock University, Nigeria for giving me the golden opportunity to be a part of them and also for molding me into who I am today. I am forever grateful.

I would also like to express my special thanks to my supervisor Mr. Karol Kornatka for his support and helpful criticism when needed. And to my Daddy, Engr. Barth C. Nwagboso for his brilliant advice and astounding support throughout the course of this project.

I also extend thanks to Mr. Osinachi Nwagboso for his tireless contribution towards the success of my project and always being there when I needed him.

I am also thankful to all others who have helped me directly or indirectly throughout the completion of my project.

**TABLE OF CONTENT**

1. **INTRODUCTION**
   1. **WHAT IS RODIX**
   2. **OBJECTIVE AND SCOPE OF THE PROJECT**
2. **ENCRYPTION OF DATA**
   1. **LITERATURE REVIEW**
   2. **WHAT IS ENCRYPTION OF DATA?**
   3. **WHY ENCRYPT?**
   4. **TYPES OF DATA ENCRYPTION**
   5. **DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC ENCRYPTION**
   6. **REASONS TO ENCRYPT**
3. **GETTING STARTED WITH RODIX**
   1. **LOGGING IN**
   2. **AFTER LOGGING IN**
   3. **LOGGING OUT**
4. **USING RODIX**
   1. **DURING YOUR SESSIONS**
   2. **HOW IS THE PASSWORD ENCRYPTED?**
   3. **WHERE IS THE PASSWORD BEING SAVED?**
   4. **HOW ARE THE NOTES ENCRYPTED AND WHERE ARE THEY SAVED?**
5. **FEATURES OF THE APPLICATION**
   1. **CHANGING PERSONAL DATA**
   2. **HOW TO CREATE NOTES**
   3. **ADVANTAGES OF RODIX**
   4. **DISAVANTAGES OF RODIX**
   5. **WHERE CAN RODIX BE USED?**
   6. **ADDITIONAL INFORMATION**
   7. **LIMITATIONS**

**6. LICENSING**

**7. SUMMARY,**

**8. CONCLUSION AND RECOMMENDATIONS**

**9. REFRENCES**

**CHAPTER ONE**

**INTRODUCTION**

Knowledge is so vast that we can trace our success from the past. History has it that the ancient Egyptians, Mayans, then the Greeks and Romans in wartime and politics were the first people to use encryption. It was used as a security practice to encode messages that can deceive the enemy. Today, it is basically the method of turning plain text information into unintelligible format (cipher), using different algorithms. These algorithms provide confidentiality and drive key security initiatives including authentication, integrity, and non-repudiation. Authentication allows for the verification of a message’s origin, and integrity provides proof that a message’s contents have not changed since it was sent. Data or plain text is encrypted with an encryption algorithm and an encryption key which only can be viewed in its original form if it is decrypted with the correct key. (Digital Guardian, 2017)

The National Security Agency (USA?) took the unprecedented step of approving a public-domain encryption algorithm, AES, for classified information processing in 2003. Good encryption algorithm strength is not enhanced by holding the design as secret but a public domain encryption standard is subject to continuous, vigilant, expert crypt analysis. Any breakthroughs will very likely be available to users as well as their adversaries at the same time. In consumer applications, this isn’t as much of a problem, but in military communication applications it can be disastrous because the adversary can have national intelligence agency level resources and can exploit vulnerabilities as soon as they are identified. If practical vulnerabilities are found, there will be a period of reduced confidence until a new algorithm can be installed. (Alan K et’al, 2010)

The usefulness of this application ranges widely; it is used to protect data in numerous areas, such as e-commerce, online banking, cloud storage, online communication and so forth. An example of a cipher can be, for instance, the replacing of the letters in a message with the ones forwarded in the alphabet. So if your original message read “Meet you at the cafe tonight” the encrypted message reads as follows: “Nffu zpv bu uif dbgf upojhiu”

Our world has changed so fast that digitalism has taken over and people hardly rely on keeping hard copies as diary. Nevertheless few people still have the tradition of keeping notes. The introduction of “RODIX” software is to help cure the infested world of computer allowing the user to encode his/her writings, rendering it impossible to view these notes with other software. It is software that doesn’t only need your credentials to log into but will encrypt your notes when saved. RODIX allows the user to write notes, making it the smartest software of its kind and it is more potable when compared to the traditional diary.

**WHAT IS RODIX? :**

It is an app created to secure notes in a more confidential way, avoiding unnecessary access to note we want to keep to ourselves

RODIX has a wide range of features from the calendar to calculator and saving account to file. RODIX can be compared to notepad in some sort of way but RODIX on its own is very unique software.

How did the name RODIX come about?

On creating the idea of the application and how it will operate I was thought of what I will call the app when I was done programming it. So the word RODIX came to my mind, my dad started a company and he named it RODIX. Although the company isn’t a computer company but I thought of expanding the idea my dad had for the company so I decided to name it RODIX.

**OBJECTIVE AND SCOPE OF THE PROJECT**:

The objectives of this project include the following:

* To examine the meaning of encryption and also Advance Standard Encryption
* To have the knowledge on the reasons data are encrypted
* To know the differences between the types of encryption
* Introducing a new application software that helps in data encryption
* Examining the content of Rodix

The main goal is to keep notes that you do not want to be quickly or easily accessed by others. This application is very user friendly and has wide application in industry, military and government.

**CHAPTER TWO**

**LITERATURE REVIEW**

The following will be discussed in this chapter: what an encryption is, encryption of data, types of encryptions, differences between the types

Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet. File, folder, can be encrypted using GnuPG or AxCrypt .Some file compression programs like Stuffit Deluxe and 7-Zip can also encrypt files. Even common programs like Adobe Acrobat and Intuit TurboTax allow you to save password-protected files, which are saved in an encrypted format.

An encrypted file will appear meaningless to anyone who tries to view it. It must be decrypted in order to be recognized. Some encrypted files require a password to open, while others require a private key, which can be used to unlock files associated with the key.

Encryption is also used to secure data sent over wireless networks and the Internet. For example, many Wi-Fi networks are secured using WEP or the much stronger WPA encryption. You must enter a password (and sometimes a username), connect to a secure Wi-Fi network, but once you are connected, all the data sent between your device and the wireless router will be encrypted. (Tech term, 2014)

There are many different types of encryption algorithms, but some of the most common ones include AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish, RSA, and DSA (Digital Signature Algorithm). While most encryption methods are sufficient for securing your personal data, if security is extremely important, it is best to use a modern algorithm like AES with 256-bit encryption. People sometimes want to write some information that they don’t want people to get direct access to. This windows application helps in keeping your notes safe from any unauthorized persons.

**WHAT IS ENCRYPTION OF DATA**

This simply means putting a password or key on a file and making it impossible for anyone to decode it. In modern times encryption is one of the widely known and effective methods of data security.

WHY ENCRYT?

CIPHERTEXT

ENCRYPTION ALGORITHM

PLAIN TEXT

People sometimes want to write some information that they don’t want people to get direct access to. This windows application helps in keeping your notes safe from the unauthorized persons.

**Types of data encryption**

* **Symmetric encryption**
* **Asymmetric encryption**

**Symmetric encryption:** This type of encryption requires only one key to encrypt and decrypt the data; it could be a key, number, word or a string of numbers. This is a widely known method and oldest type of encryption.

**Symmetric Key block ciphers**

Just to mention a few common key block ciphers like:

* Advanced Encryption Standard (AES): It is a symmetric encryption algorithm; it was developed by Joan Daemen and Vincent Rijmen, two Belgian cryptographers. It was designed to work in hardware and software efficiently which supports a block length of 128 bits and key lengths of 128, 256 and 192. AES was adopted by the U.S government but is now used by different nations. It was first published in 1998 and it supersedes Data Encryption Standard.
* Data Encryption Standard (DES): It is also a symmetric key algorithm which was developed in the early 1970s at IBM and first published in 1975 and standardized in 1977. It encrypts electronic data. It was highly used in the development of modern cryptography but now considered insecure.
* Blowfish: Another symmetric key algorithm which was designed by Bruce Schneier in 1993 and also published in the same year. It supports block size of 64bits , key size of 32 – 448 bits

COMPARISIM BETWEEN AES, DES AND BLOWFISH

* DES is very old and has short key sizes for efficient security
* AES is the successor of DES and accepts keys of 128 bits which is very unbreakable.
* Blowfish has a key size from 32- 448 bits and it is very efficient in software.

So, if you are ever in doubt of which one to use AES is much more preferable to use. Remember that block cipher encrypts blocks and if your message is more than 128 bits the message will be split into blocks. This is called chaining or mode of operation.

**Asymmetric Encryption**:This type of encryption requires two keys one to encrypt the message and one to decrypt the message. The issue with this type is that while exchanging the keys online it may fall into the wrong hands. However, two keys are made a public key in which you can make available to anyone and a private key that only you will have.

**DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC ENCRYPTION**:

* Asymmetric takes longer time than Symmetric Encryption.
* Asymmetric is new while Symmetric Encryption is old.
* Symmetric is one way while Asymmetric is two ways.
* Symmetric uses one key to encrypt and decrypt and Asymmetric uses one key to encrypt and the other to decrypt.

**REASONS TO ENCRYT:**

* To prevent valuable data breach.
* To safeguard data when sending it through email or cloud.
* To ensure the authenticity of the data.

**2. GETTING STARTED WITH RODIX**

A quick guide on the types of login sessions using RODIX.

SETTING UP

Setting up RODIX is quite easy. When installing the program you have to run the setup as administrator. Follow all the steps required and you select where you want your program to be installed in. When you’re done installing the program you're also required to run the program as administrator.

**2.1 LOGGING IN**

After you launch the program, you will be asked to log in with a name and password. Obviously you’re new to the application so you have to create an account. Here you will be asked to input:

* A name (which will be your log in name)
* A password of your choice
* Recovery question with an answer in case you forget your password after creating an account.

Archiving all these you will be able to log in. There is also a platform in case you forget your password, and here you will be asked to input your name and the answer to your recovery question. Doing that correctly you will get back your password.

**2.2 AFTER LOGGING IN**

You will be presented with a login message before you enter the dairy. After you’re logging in into the dairy; whatever note or content you decide to put in is totally up to you.

**2.3 LOGGING OUT**

When you are done with writing your notes and want to leave the application; just click on the tab button then you will see a logout button. You will be shown a message to confirm if you want to logout or not but confirming will close the program.

You can close it by using the CLOSE button in the window border. But this isn’t appropriate although it will not cause any harm to the application- a bit like shutting down a laptop. Its better clicking shut down than holding the power button down to switch off. I recommend logging out through proper means and you do not have any other way to close it.

**4. USING RODIX**

This chapter will help provide an introduction to the features of RODIX, how files and your password are encrypted.

**4.1. During your session**

Once in you can create, rename and delete files. There are also more features to be identified later in this chapter.

**4.2. How is the password encrypted?**

The password is encrypted and then mixed with the username and other useful data for the program using an algorithm and then saved to a file. It is saved with other files in a table that is later encrypted by a secret algorithm.

DISGUISE PADDING

INPUT PADDING

ENCRPYT WITH METHOD 2

ENCRPYT WITH METHOD 2

ENCRPYT WITH METHOD 1

NORMAL TEXT

**REVERSE REVERSE**

**REVERSE**

**4.2.1. Where is the password being saved?**

The password of an account is saved on a supporting dynamic link (.dll) file that is in the parent directory of RODIX.exe

**4.3. How are the notes encrypted and where are they saved?**

The notes are encrypted with an algorithm that converts the data to UTF8 bytes and the bytes are then converted to base64 string format and then it hides its padding sign with other symbols or letters like “?” or "AAAAAAAAAA" so the encryption method won’t be obvious. The files are saved in the folder named “20” in the user folder.

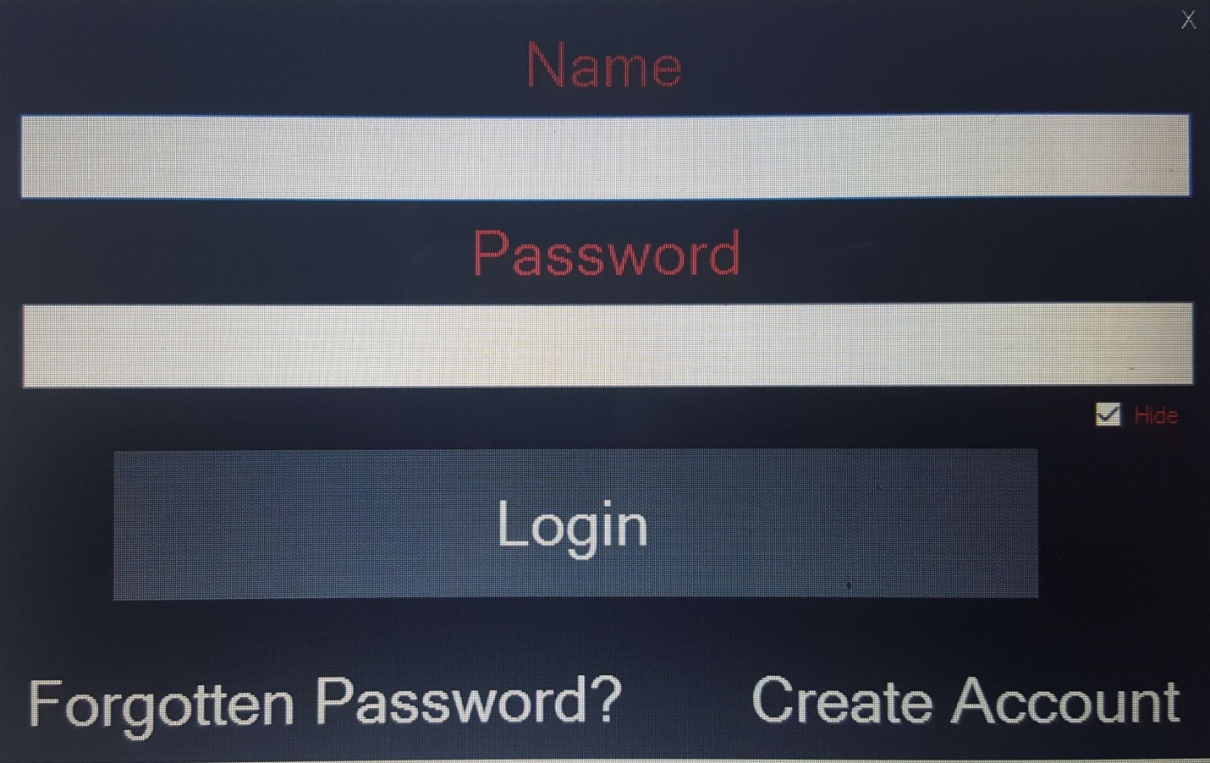
**5. FEATURES OF THE APPLICATION:**

**The interface:**

**The red and black interface or mostly known the red /black concept simply refers to careful separation of classified plain text (red signals) to cipher text (black signals)**

CIPHERTEXT

PLAINTEXT

****

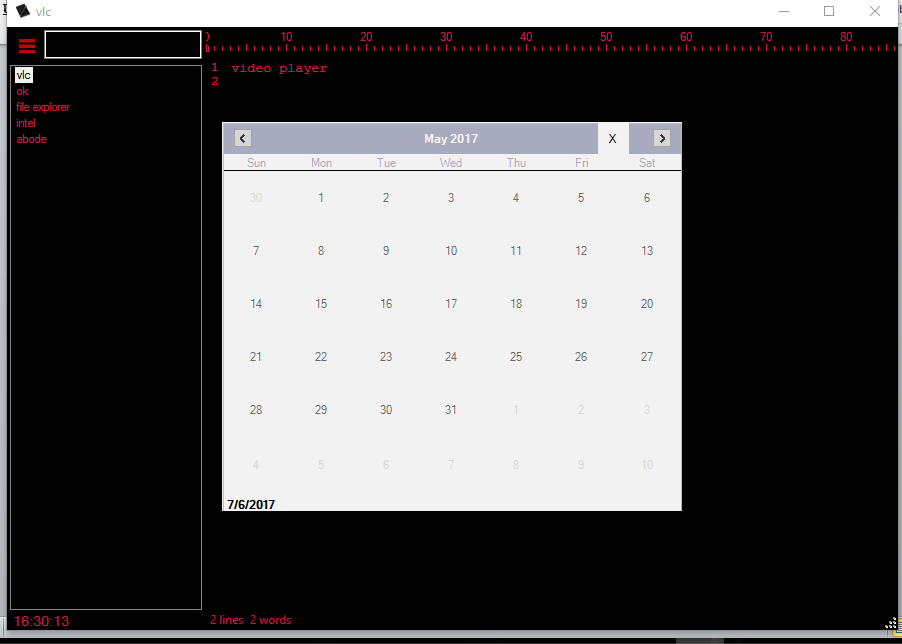
* As most modern applications it allows multi users
* You are given the option to recover your password if forgotten (Image below):

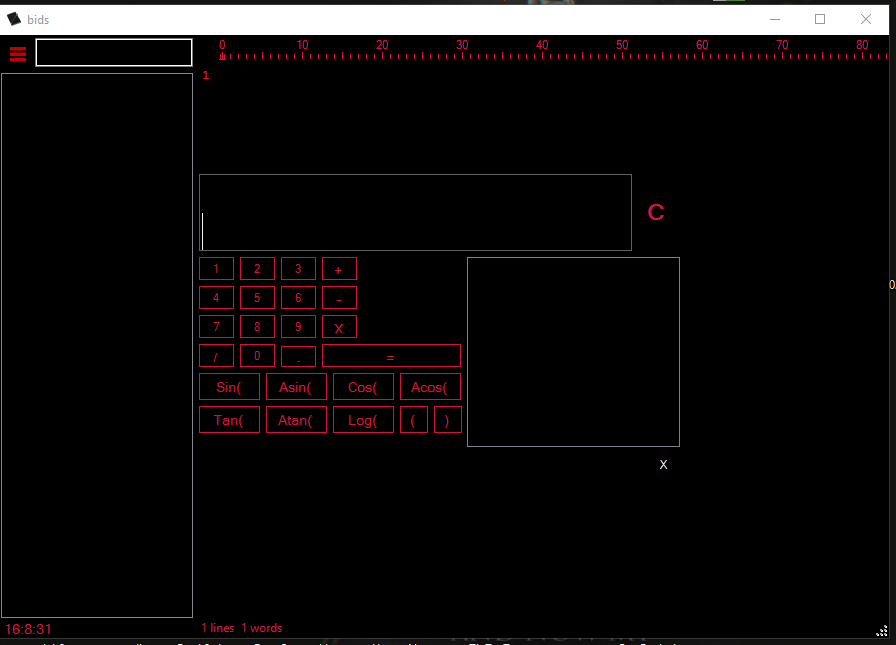


You’re the only one who knows your secret question and answer. You show your password if you forget to input your name and the answer to your question. On clicking resolve it will show you your password.

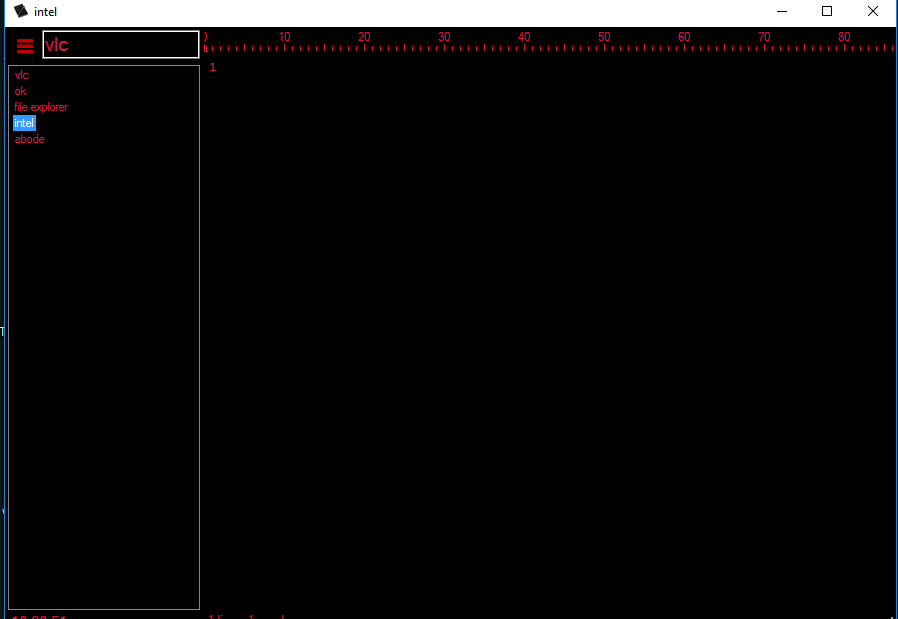
However it is also possible some people also forget their secret question hence rendering them unable to put in the correct answer. When you put in your name it will display your question and reminding you of your answer. (Note: the harder your answer is, the harder it is for people to log into your account).

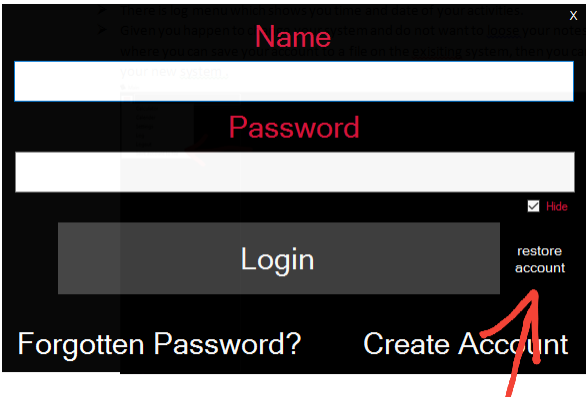
* There is a time, calculator and calendar if needed(Image below)



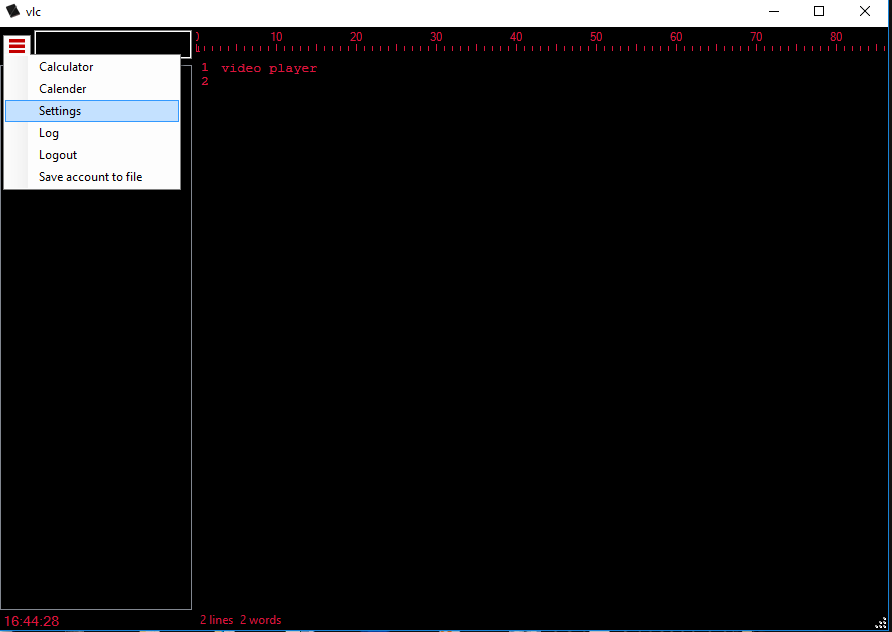
.

* It has margin lines just like MS word( i.e. you can know which line and how many words you have written )
* You have the ability to search for notes quickly (i.e. If you have created lots of notes. Image below)

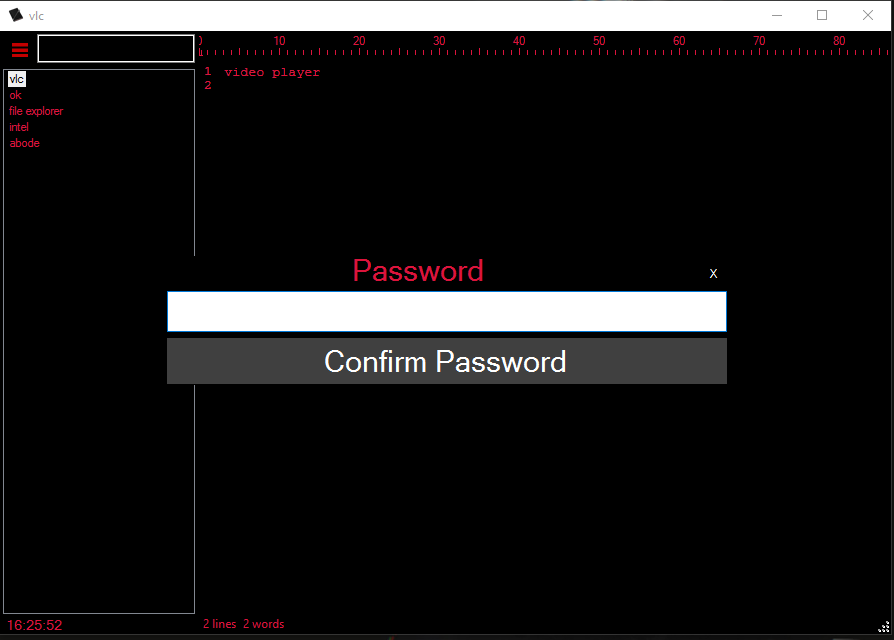


* There is log menu which shows you time and date of your activities.
* Given you happen to change your system and do not want to lose your notes there is a feature where you can save your account to a file on the existing system. Then you can copy this file to your new system.
* On starting up the program on a new system all you need to do is click the option to recover your account and the program will open a file explorer and you will go to the directory of where you copied the file to.

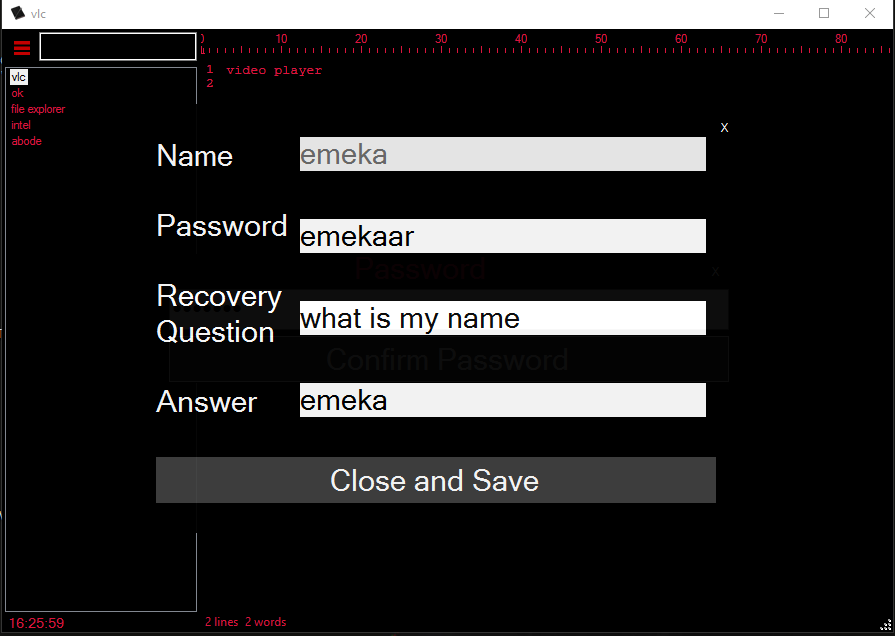
5.1. CHANGING PERSONAL DATA :



The figure above shows the menu to go when you want to change your account settings.



Your password must be out in correctly before you can access your personal information.



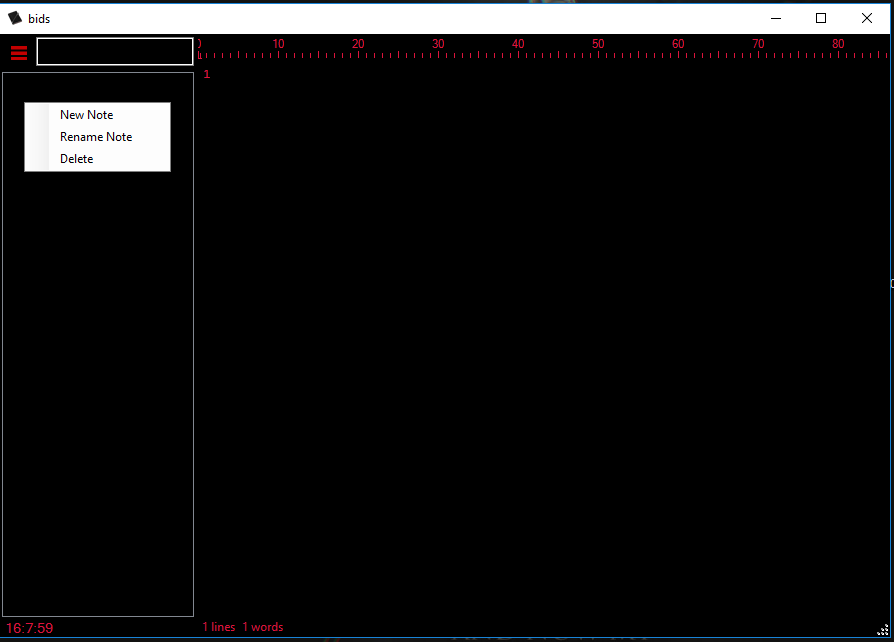
The figure above shows your account details and you can change your data and save when you’re done.

5.2. HOW TO CREATE NOTES:

To create notes to go to left side of the application under the search bar. You right click and three options will be given to you:

* New note
* Rename note
* Delete

NOTE: whenever the application is being run, you must run it as administrator in order for these features to work.



5.3. ADVANTAGE OF RODIX:

* Its hidden meaning notes that are saved in RODIX are not accessible outside the RODIX environment
* It is an offline application; it has not direct access to the internet yet so internet scammers and hackers cannot use the internet to decrypt your notes.
* Each activity is recorded, with exact time and date.

**5.4. DISAVANTAGES OF RODIX:**

* If the codes used to write the program are accessible to a hacker it is easy to decrypt notes. (N.B the codes are only accessible by the owner of the program and will not be shared with any user of the program).
* Case sensitive (during account creation).

5.5. WHERE CAN RODIX BE USED? :

* Refinery or Power Plants: Readings are taken during operations in both places. These could be temperature, pressure, current, volume, etc. People are in charge in the control rooms to record these readings. If these readings are unfortunately exposed to evil minds, then it could expose the plants to sabotage and untold damages. . RODIX is a good program to store your plant operations readings in.
* Research Laboratories (Medical field): New researches are done in medical fields; new drugs are made to help fight diseases. Scientists and doctors make researches and formulas are derived in making new drugs. Imagine having a competition with another company to release a particular drug for a specific disease you don’t want your formulas and notes to be released to your competitors. Because of market economy and other factors, tension will be between the companies and each will want to be the first to release the drug. The world is going digital and most scientists and doctors will want to save their notes on their computers plainly (if the computer is breached it’s easy to get information) RODIX can help keep your research safe from others.
* Military (Internal & External Security): Everyone knows what it means for documents to be classified. RODIX can help protect some information hidden from officers who do not have authority to view it.

5.6. ADDITIONAL INFORMATION:

Stable release: Windows systems; RODIX best works in a windows environment. Meanwhile, in a Linux environment the program is not yet stable.

RODIX is written in C# language.

RESOURCES:

The resource used for designing this project is Visual studio 2015;

* Visual studio 2015 is an IDE used for developing editing and debugging apps.
  1. **Limitations**

The software only encrypts notes that you create and input data in, for the software cannot encrypt note created outside this software and multimedia files like pictures, videos or audio files.

**6. LICENSING**:

Copyright (c) 2017

Permission can be granted to any person by first contacting the author, Mr. Chukwuemeka Chinedu Nwagboso

Of this software and associated documentation files (the "Software"), to deal

In the Software without restriction, including without limitation the rights

To use the software.

However users are not allowed to copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software to anybody, subject to the following conditions:

The above copyright notice and this permission notice shall be included in

All copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHOR OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**7. SUMMARY**

This project is aimed at designing and implementing an encrypted dairy which helps in improving the privacy and security of users who still want to be keeping notes digitally. From the statistics of those that have tested the project, it is safe to say that the use of the application improves privacy and authencation of user’s notes.

**8. CONCLUSION AND RECOMMENDATIONS**

The world of computers and Mathematics are really growing rampantly now and people should take good use of this and educate themselves more on how it could be of advantage to them

The software can help save a lot of people hacking , petty stealing and outrageous amount of money paid to get secured servers to store information only you want to have access to.

In conclusion the project has vividly explained ,designed and implemented an application that save and encrypt notes.

The applications can used by almost all areas of life and profession where the need to keep notes hidden from preying eyes are desired. The software can be used by the government, oil companies business for simple storing of notes.

**9. REFERENCES**