

Requirements Specification

Version 1.0

Version History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date | 10/21/2009 | Authors | Anthony Sinatra  Dmitry Sharlot  Joseph Everett  Ricardo Viera | Version | 1.0 |
|  | 10/25/2009 |  |  | Created specification overview | |
|  | 10/27/2009 |  |  | Updated with details after implementation meeting | |
|  | 10/27/2009 |  |  | Updated with Operation, Security , Maintainability, and Portability requirements | |

Table of Contents

PROJECT DRIVERS

1. The Purpose of the Product

2. Client, Customer and other Stakeholders

3. Users of the Product

PROJECT CONSTRAINTS

4. Mandated Constraints

5. Naming Conventions and Definitions

6. Relevant Facts and Assumptions

FUNCTIONAL REQUIREMENTS

7. The Scope of the Product

8. Functional and Data Requirements

NON-FUNCTIONAL REQUIREMENTS

9. Look and Feel Requirements

10. Usability Requirements

11. Performance Requirements

12. Operational Requirements

13. Maintainability and Portability Requirements

14. Security Requirements

**1.)Purpose of the Project**

Many people communicate with one another using electronic mail. Most people believe that their communication remains secure; however, this is not the case. These electronic mails travel over many networks in order to reach the intended recipients. These networks may exhibit security flaws and various vulnerability points, which could compromise the user’s data.

Communications and/or data which has been intercepted during transit should remain restricted from use by a third party. The FogWire application will enable the user to secure his/her electronic mails prior to sending. Only verified users will be able to unlock these electronic mails upon receipt.

**2.) Client, Customer and Other Stakeholders**

2.1. Our client is the general public.

2.2. Our customer is any person who sends electronic mail and would like to ensure that it is sent securely.

2.3. Other stakeholders:

Pace University and Professor Marchese have provided the initiative for the development of this product.

**3.) Users of the Product**

Most people believe that their electronic mail communication remains secure, while it in fact does not. Once this issue is realized by general public, there will be larger demand for this type of system. Our user base will be anyone who currently communicates via electronic mail; such as teenagers, young adults, adults, and in many cases even seniors. Our target age range would be 13 and up.

**4. Mandated Constraints**

This application will require that the users’ computer is connected to the internet.

**5. Naming Conventions and Definitions**

Encryption – the process of transforming data into an un-decipherable form by using algorithmic functions.

Decryption – the process of de-coding data from its encrypted state

User – anyone who will utilize this application for the purpose which it is intended.

Electronic Mail – data which is sent electronically over multiple networks using electronic mail servers and a personal computer (PC)

**6. Relevant Facts and Assumptions**

The user should understand the implications of encryption and decryption of data, which means he/she should know that once data has become encrypted, it must be decrypted in order to be useful in any way to the recipients

7.)Scope of the Product

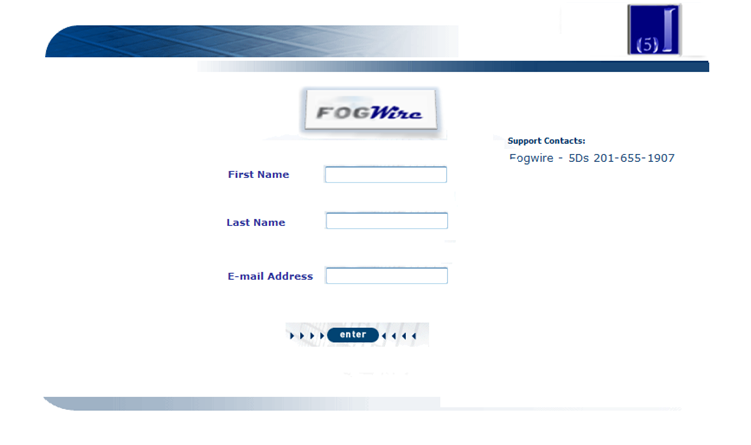
* + Users require the ability to setup a user profile within the application.
  + The user profile will authenticate each user in order to verify whether he/she should be given access to lock and/or unlock data communication.
  + Users require the ability to securely communicate with one another.
  + Users need to securely transfer data from one authorized user to another while restricting unauthorized access to the data.
  + If data interception occurs, the data should remain unusable by another party.
  + Users need to obtain and utilize protected data which has been sent from another authorized user
  + Users will send this protected data via an electronic mail client.

8.)Proposed Functionality

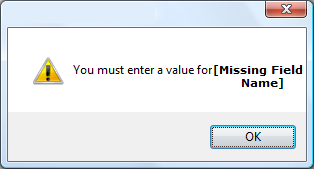
8.1) User profile setup

When users launch the application for the first time, he/she will have the ability to setup a user profile. This profile will store information about the user:

1. First Name
2. Last Name
3. E-mail Address
4. Unique Authentication Key (**Note:** This data point will not be displayed to the user. It will be stored in the database and will be created by the application)



Note: All Fields are required. User cannot save a profile if any of the fields are incomplete. If any of the required fields have been omitted, the user will receive a warning:

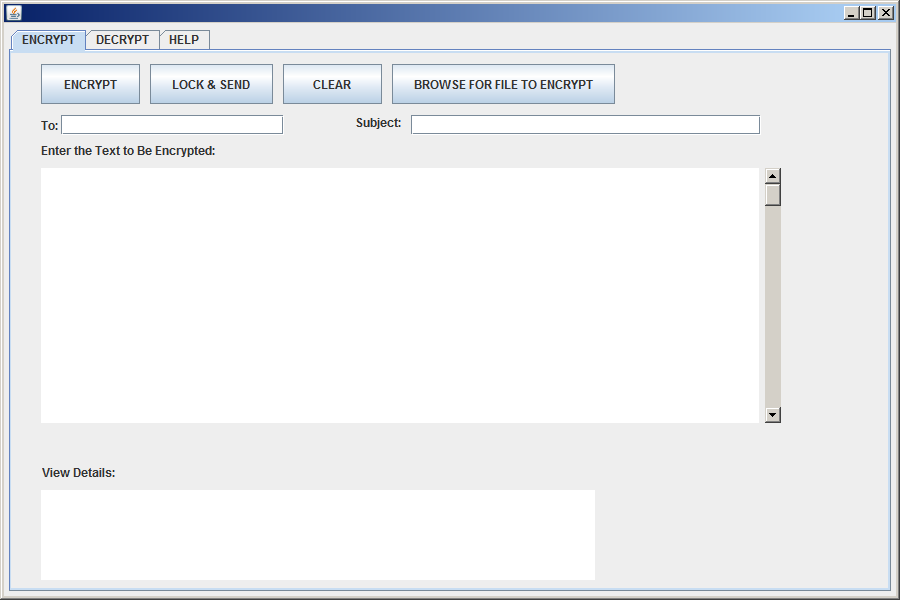


After the data has been entered, the application will connect to the FogWire database server in order to store the information which has been entered. The user’s private key and public key will be generated by the system and stored in the database with the user’s information.

**Note:** The users’ private and public keys will not be communicated to the user.

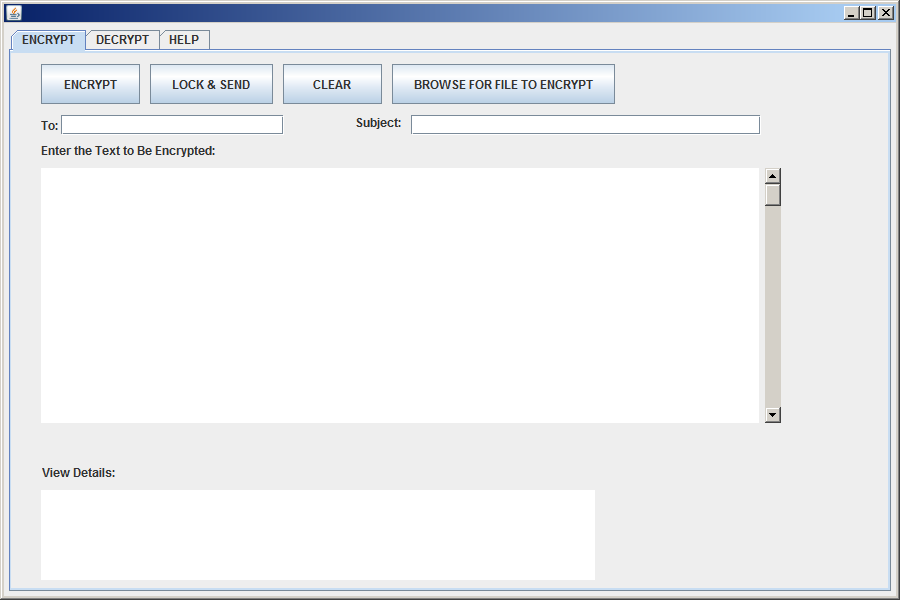
8.2) Securing Data

After the user has setup his/her profile information, he/she will access the application. In this area, the user will be able to free-type data into the text box or select a file to secure.



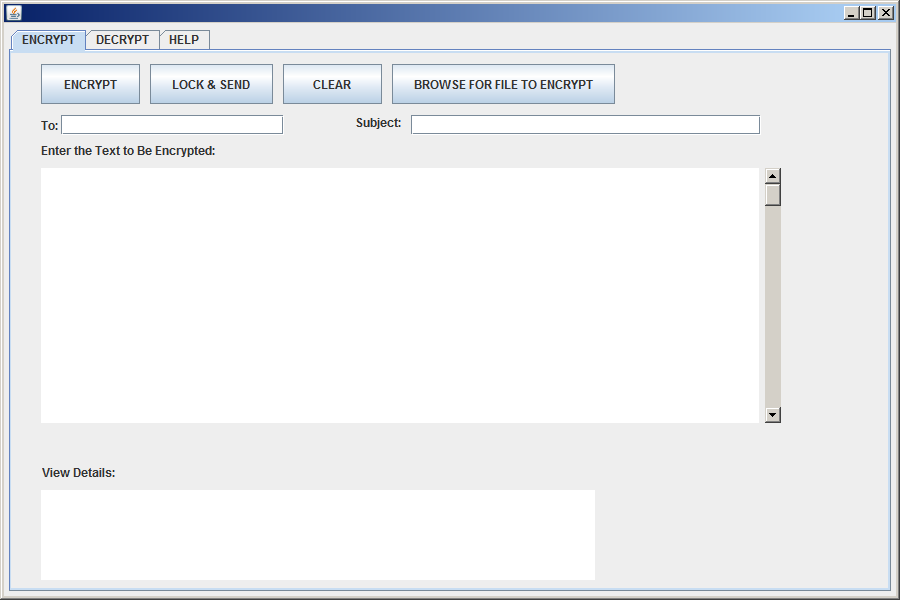
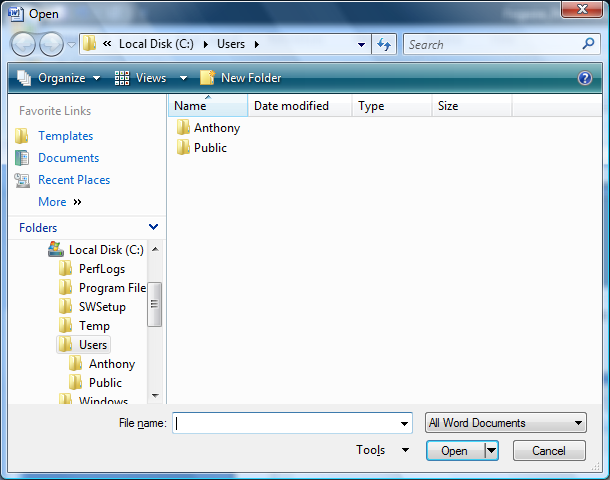
a.)The encrypt tab will be selected by default after the user has opened the application.

b.) If the user selects to type data into the ‘Enter the Text to be encrypted’ area, the ability to browse for a File to encrypt will be disabled.



c.) User can free-type text and/or cut and paste text from another word processing application into the text box.

c.)If the user selects to browse for a file, a prompt will appear which allows the user to select a file from using a standard file selector:



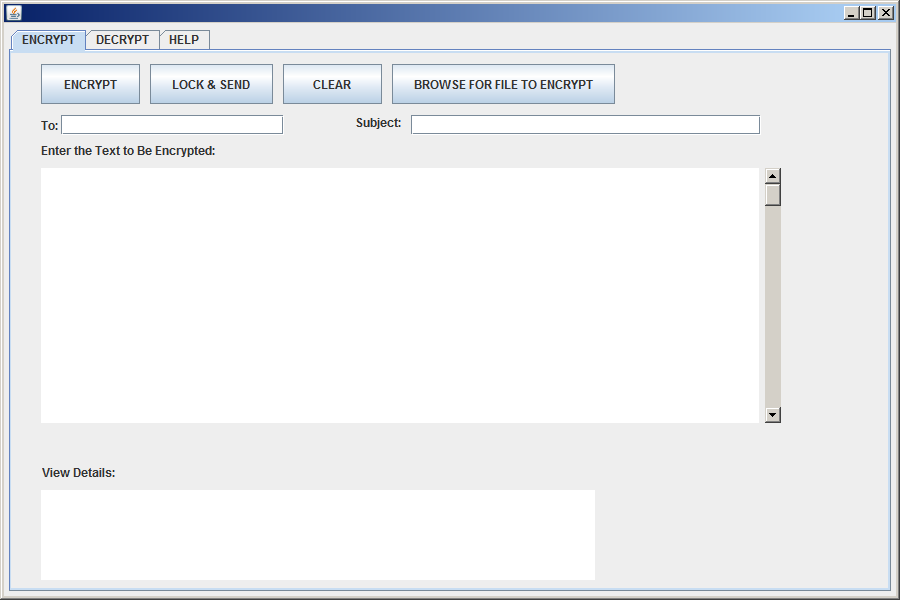
The file selector will default to the users’ C:/ drive.

d.) After the user has selected a file or entered information into the text-box, he/she can select to:

1. Encrypt
2. Lock and Send
3. Clear

8.3) Encryption

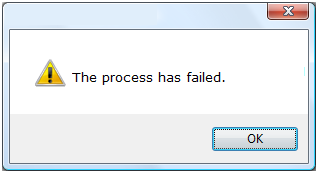
Data entered into the textbox or the file selected will become encrypted after the user selects the ‘Encrypt’ button. The encryption process will transform the data or data file into an encrypted file which would be completely undecipherable – unless both corresponding Private and Public keys are available. The encryption process will insert the private key of the user into the data at each encryption point. This will allow the ‘Decryption’ process to unlock the data. **(Decryption process will be described in section 2.5)** The encrypted file will be stored on the users’ computer in a FogWire application folder > Locked Files



After the encryption process has been successfully completed, the user will receive a message which informs he/she that the process was completed successfully.

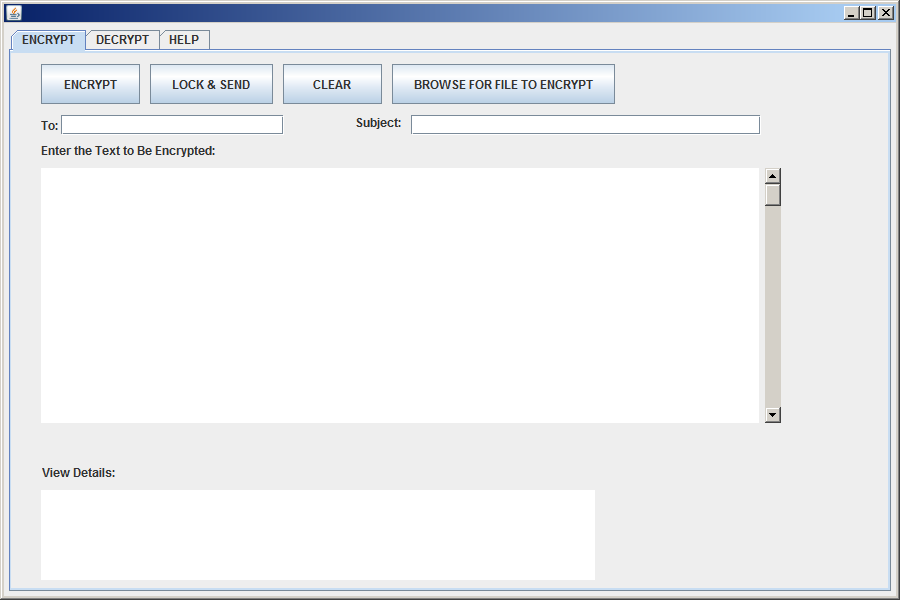


If there is a problem with the encryption process, the user will receive a message which states the process has failed.

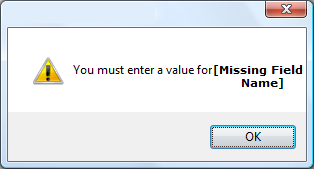


8.4) Lock and Send

Lock and Send will follow the same process described above; however, there will be an additional step. The user will send the encrypted file to another FogWire user. The user will enter the recipients e-mail address into the ‘To:’ field and the subject in the ‘Subject:’ field. Both fields are mandatory when the user selects ‘Lock and Send’.



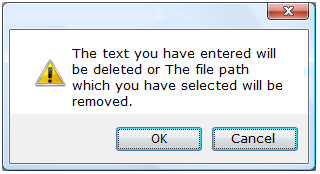
If either ‘To:’ or ‘Subject:’ is missing and the user has selected ‘Lock and Send’, the user will receive a warning message .



The encrypted file will then be sent to the recipient using the from e-mail address which has been stored for the user of the application. The e-mail body will contain a message “You have received a message from another FogWire user. Please open the file using the FogWire application in order to unlock the data”. The encrypted file will be an attachment to the e-mail.

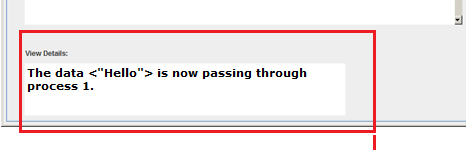
8.5) Clear

When the user selects ‘Clear’, the text box will be emptied of all the data which has been entered. If the user has selected a file, the file path will be cleared. The user will receive a warning message:



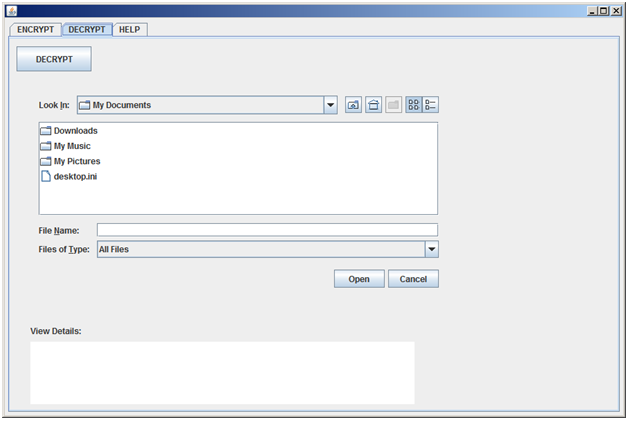
8.6) View Details

The user can select to view details which will display the encryption process to the user on the interface. The detailed steps of the encryption process will be explained to the user:

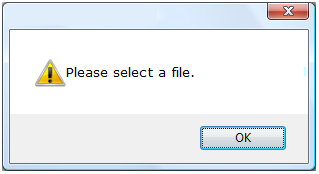


8.8) Decryption

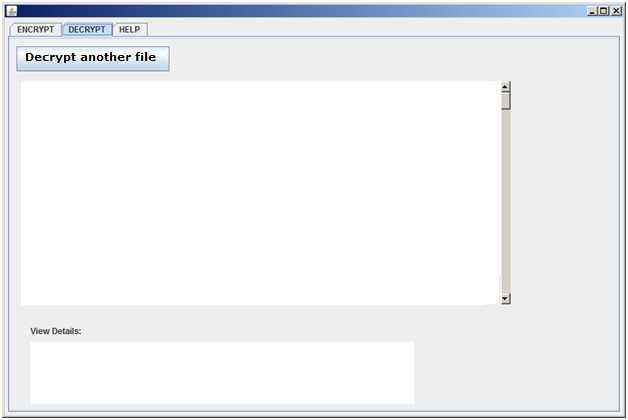
In order for the encrypted data to be unlocked, the recipient of the encrypted file **must** open the file using the ‘Decrypt’ area of the FogWire application.



The user can select a file which he/she would like to decrypt (unlock). If the user does not select a file and he/she selects ‘Decrypt’, a prompt will appear:



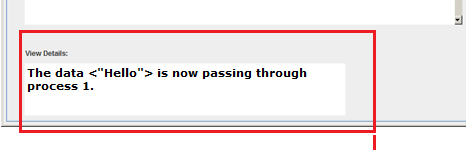
Once the file has been decrypted, the text will display to the user:



The user can also select to ‘Decrypt another file’ which will bring the user back to the file selector screen.

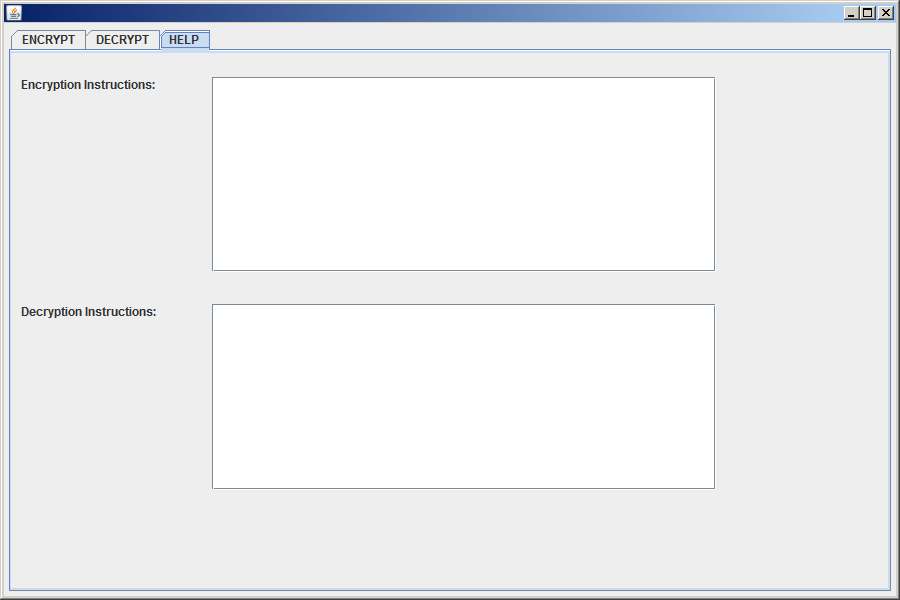
8.9) View Details (Decryption)

The user can select to view details which will display the decryption process to the user on the interface. The detailed steps of the encryption process will be explained to the user:



8.10) Help

This help area will display quick instructions to the user on how to perform any relevant actions in FogWire system.



8.11) Implications

The application will not function properly unless the user is connected the internet. The application **must** have a connection to the database in order for the system to verify and/or store the users’ information.

8.11) Database

Store the following data points:

1. First Name
2. Last Name
3. E-mail Address
4. Unique Private Key
5. Public Key

9. Look and Feel Requirements – Joe/Anthony

10. Usability Requirements- Joe/Anthony

**11.)** **Performance Requirements**

This section identifies criteria for system response to user initiated events such as the speed of encrypting data, decrypting data, accessing data on the server for ad hoc queries, sending data via email client and browsing through the application.

To date, no requirements for performance have been identified. However, the above specified user initiated events should be accomplished in a reasonable time frame in line with industry standards.

**12.) Operational Requirements**

General Description of Operational Capability

* 1. Mission Area Description

FogWire is a security software used to hide messages from unintended recipients. The software is intended for single users accessing files and or documents on their computer consoles.

* 1. Mission Need

Messages that are intercepted by third party users may have valuable information not intended for the third party to read. This need for secrecy is the purpose of FogWire, which is to mask important messages from prying eyes and make them unreadable.

* 1. Description of the Proposed Product or System

FogWire will open a message from file or allow a text message to be created within its software interface, with the receiving of a message or sending it. The masking of the message addresses the problem of outside parties reading unsecure important data and performs the task of keeping a user’s message secret.

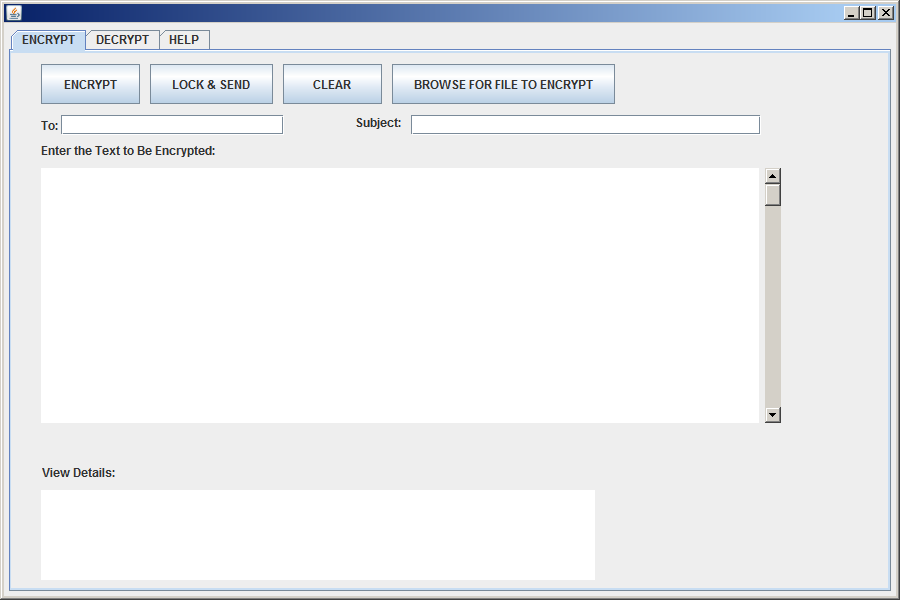
* 1. Mission the Proposed System will Accomplish

FogWire will allow a user to mask their message by form of encryption and make it unreadable. The message will then be allowed to be open only by the intended recipient.

* 1. Operational and Support Concept

The System will encrypt a message with a public recipient key. The recipient will open the message using the private inverse version of the encrypted key. The recipient and only the recipient has the private key therefore only the recipient is able to decipher the encrypted message.

Both recipient and user will work with their intended messages via FogWire software interface.



12.6 Threat

The intended threats are hackers, users with network listeners that may receive message from senders with the purpose of reading them. If and when the users message is compromised the message is indescribable to anyone except its intended recipient.

* 1. The System shortfalls

User may not be able to encrypt any file , ie .pdf, .doc. The software is intended for text up to the end of the entire software creation phase. Therefore, without more time than currently allowed the software is intended for text messages.

* 1. Capabilities Required

Fogwire will complete its tasks by having an encrypt/decrypt function, a text area, and a send function. The encrypt function will apply the algorithm that will mask the message. The Text area will display the original message or show the new message being created. The send function is used to send the encrypted message to another user via email.

Fogwire must encrypt a message and decipher this message back to its original form at the minimum the message is of extension .txt. Fogwire should allow this message to be sent to a recipient via email.

* 1. System Support

The software is fully functional upon receipt. It is also easy to use with instructional document attached.

* 1. Maintenance

FogWire is self maintained.

* 1. Supply

FogWire is software that may be used on a PC. The software can be ran on any pc by simply copying the initial software and installing it. Tools and or supplies are not necessary.

* 1. Support Equipment

FogWire will have an email for problems and or questions to the system for continued FogWire software improvement and development of newer versions.

* 1. Schedule

System will be available by the end of the Software Engineering I course at Pace University by December 23, 2009.

* 1. Cost

The system will be made available to Professor Marchese and current 5d partners. It will be free for them. The target price will be negotiated after the completion of the project and the course at Pace University Software Engineering I (fall 2009).

**13. Maintainability and Portability Requirements**

13.1) Maintainability

This section identifies efforts required to locate and correct an error during operation.

Our application is simple to use and intuitive/easy to learn. The excellent documentation and simple to follow code provides for seamless transition of maintainability between different parties. As a general metric, for a 20% increase in functionality of the software, we are estimating a 4 week turnaround. Maintainability will decrease over time as more and more functionality is delivered. Additional maintenance is required as the application itself will increase in size.

13.2) Portability

This section identifies efforts needed to transfer from one hardware or software environment to another. Our application is expected to run under Windows 95/NT/XP/VISTA/7 as well as UNIX.

**14. Security Requirements**

General Security Hazards

The scope of FogWire security is within the individual’s computer console. Fogwire is not accessible on the internet and or server. It is software to be run on an individual console. The Security for the console is up to the individual.

The User’s information will be encrypted depending on the recipient whom the user is sending a message. That is, if the user is sending ten different messages to ten different users then each message is encrypted using the ten different public keys available by the recipients via key distribution center on a server. The user’s personal information may also be encrypted provided the user performs that particular function.

FogWire performs a task of security as a product and therefore under the product description has an explanation of the software’s functionality.