A consumer focused encrypted communication software should take into account the following factors when designing the user interface:

- The users have to be made aware of the security tasks that they have to perform.
- Are able to figure out how to successfully perform these tasks
- Don't make dangerous errors
- Are sufficiently comfortable with the interface to continue using it

(Ref: Alma Whitten and Doug Tygar)

The email client I used "gmail", did not have a built-in encryption software and I did not use the email client available with GPG tools (I am not sure if any is available). In order to encrypt, GPG software was downloaded and shortcuts were added to the keyboard shortcut feature for encryption, decryption, signing and verification. First, a private (with passphrase protection) and public key was generated. There is an option to import public key or search for a public key in the user interface of GPG software. The steps to be performed to encrypt an email is not evident and a manual or tutorial was needed to perform the above tasks as well as the tasks below.

First, an email was signed with the private key of the user sending the email and then encrypted with the public key of the recipients of the email. The signature and encryption was apparent in the text, though the implications of signing first and then encrypting or encrypting first and then signing is not explicit or conveyed through the software. Also, if a signature is required or not is also not apparent. After sending the encrypted email, the recipient has to decrypt the message using his/her private key. An encrypted message received should first be decrypted using the receiver's private key and then the signature has to be verified to make sure that the signature is of the sender using the sender's public key. Opening the email without verifying the signature could lead to viruses or unverified information to be trusted. There are options to choose the public key to verify the signature and the prompt message of verification of signature successful is useful to understand the procedure. But these steps are not very clear without reading the manual or the tutorials and one could see how a user without knowledge about security could oversee many things and lead to security breach or infection with viruses or trusting of malicious or incorrect information. The interface is very minimal and understanding the implications of security breach would enable users to continue using the software though significant improvements can be made like providing a step by step tutorial in the actual software with the input of a message or text from the user. The software could ask questions like, do you want to encrypt/decrypt, sign/verify at each step which would make the software more user friendly. I would also like to add that I was not aware of the security implications of encryption and decryption prior to this assignment and was made aware of these things due to the class and tutorial rather than by the software.