# FGP (Good Privacy) - User Manual

A program for encryption and decryption of text based messages. FGP utilises a random number generator, which passes all the statistical diehard battery tests, in combination with a secure password. A secure password has more than 12 upper and lower case characters. These features makes brute forcing FGP take years, even with a super computer.

Contents

[Registering Your Product 3](#_Toc441679281)

[Using FGP 3](#_Toc441679282)

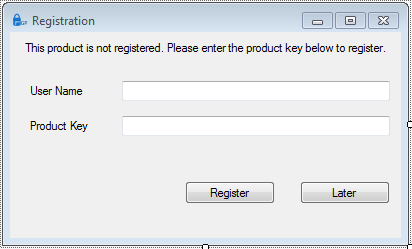
[File Encryption 4](#_Toc441679283)

[Passwords 5](#_Toc441679284)

[Fake Messages 6](#_Toc441679285)

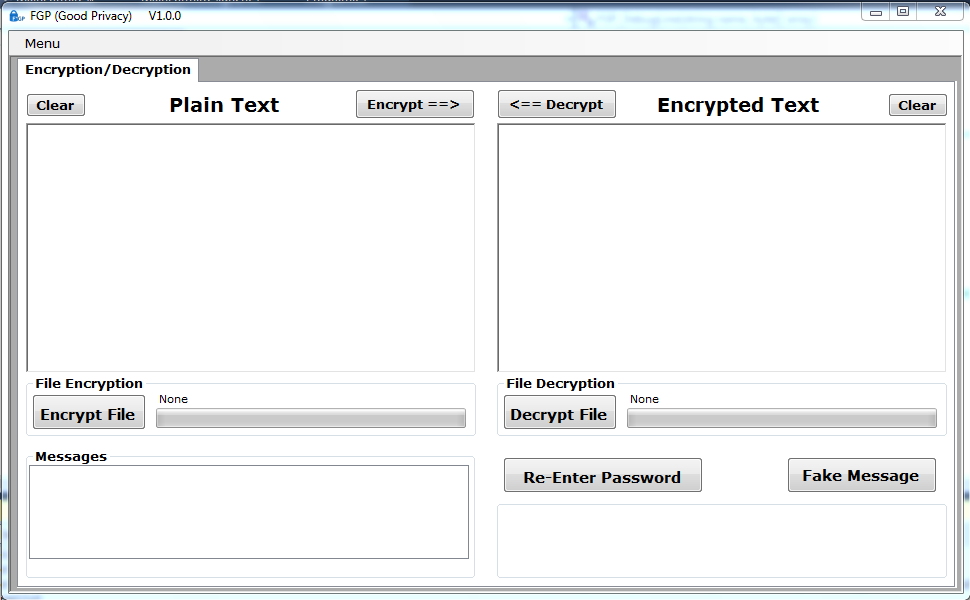
## Registering Your Product

When first using FGP, a registration window will appear. Enter the required username and provided product key to gain access to FGP.



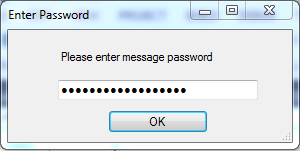
## Using FGP

The FGP main window is shown below. This can be used to encrypt/decrypt entered messages or small .txt files. Messages can be typed directly in to the ‘Plain Text’ box seen on the left hand side of the window below.



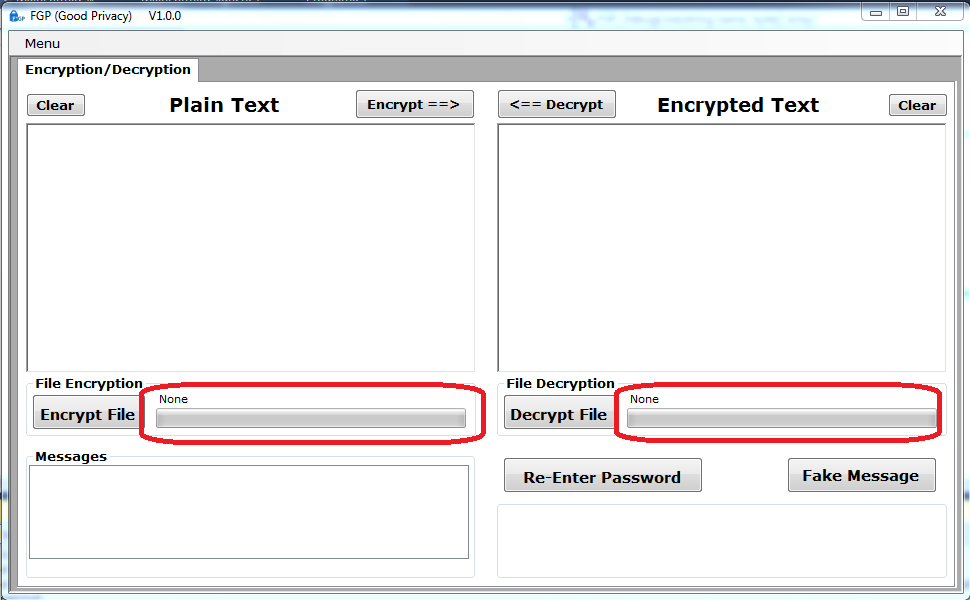
Once a message has been entered in the plain text box, the user selects the button.

The ‘Enter Password’ window shown below will then pop up. This allows the user to choose a password for message encryption. Good password design and how to change your password is described in detail in a later section of this manual. This password will be used for any subsequent encryption and decryption during this FGP session unless the user takes steps to change the password.



After the user clicks OK, the encrypted message will appear in the ‘Encrypted Text’ box on the right hand side.

If the user receives an encrypted message, they can paste this message in to the   
‘Encrypted Text’ box on the right hand side and select the  button. This will decrypt the message using the previously entered password, and plain text will appear on the left hand side. The encrypt and decrypt processes take approximately 1-5 seconds and the progress of each shown using either of the two progress bars indicated below.



Each window has a C:\Users\Janet\Documents\Crypt\Images FGP\ClearButto.png button above it. Pressing this will remove all text from the associated window.

File Encryption

To encrypt a file, select the C:\Users\Janet\Documents\Crypt\Images FGP\encryptFileButton.png button. This opens Windows File Explorer to select a .txt document. .txt format is the only supported file type for FGP. Once the file is selected, it will be saved with the same title and a .crp suffix. The progress of the encryption will be shown in the same encryption bar used for simple message encryption.

To decrypt a file, the user selects the C:\Users\Janet\Documents\Crypt\Images FGP\decryptFileButton.png button. The user must then decide what title and location the file should be saved as, before selecting the file to be decrypted. Again, the progress of the decryption will be shown in same bar used for simple message decryption.

## Passwords

Passwords are used for encrypting and decrypting messages. The first password entered will be used for any following encryption/decryption of messages unless the user changes the password using the Re-Enter Password button shown below. The Re-Enter Password simply opens the password window that appeared when first attempting to encrypt or decrypt a message.



FGP is only as secure as the password and so for password generation we recommend:

* Length over complexity – the longer a password is, the more permutations an attacker must attempt to read your message. 16 characters is a good minimum to aim for.
* Multiple unrelated words – every language has a finite vocabulary. A rule of thumb is that most people have a working vocabulary of about 10,000 words.
* Keep it simple to remember – using upper and lower case characters, numbers and punctuation symbols can be a waste of time, particularly if they make the password hard to remember. A single capital letter does increase the password permutations, but if it is the first character of the first word, that will be the first thing an automated password search will try. Adding a three letter word to a 12 character password increases the permutation count more than using upper case characters.
* Use memory aids. Phrases that can be remembered easily with a unique twist such as switching one or two words to another language are ideal.

For more details on how to generate a good, secure password, see the FGP Technical Notes.

Fake Messages

A fake message can be generated by pressing the C:\Users\Janet\Documents\Crypt\Images FGP\FakeButton.png button. This allows users to create gibberish messages to throw off any unsuspecting hackers. Fake messages are just a random length series of random numbers.